



Escuela Superior
de Ingeniería

ESCUELA SUPERIOR DE INGENIERÍA
GRADO EN INGENIERÍA EN INFORMÁTICA.

PROYECTO DE MONITORIZACIÓN DE LA GESTIÓN DE SISTEMAS Y REDES DE LA EXCELENTÍSIMA DIPUTACIÓN PROVINCIAL DE CÁDIZ

AUTOR: BRAULIO PAREJA MANZANARES

Cádiz, julio 2017



Escuela Superior
de Ingeniería

ESCUELA SUPERIOR DE INGENIERÍA
GRADO EN INGENIERÍA EN INFORMÁTICA.

PROYECTO DE MONITORIZACIÓN DE LA GESTIÓN DE SISTEMAS Y REDES DE LA EXCELENTÍSIMA DIPUTACIÓN PROVINCIAL DE CÁDIZ

DIRECTOR: CARLOS RODRÍGUEZ CORDÓN.
AUTOR: BRAULIO PAREJA MANZANARES

Cádiz, julio 2017

A todas las personas que me animaron para realizar y terminar la ingeniería.

A EPICSA por brindarme la oportunidad de realizar el proyecto y en especial a Manolo Añón Rodríguez, ya que sin él, este proyecto no se hubiera llevado a cabo.

A todos los profesionales que han participado

A Carlos Rodríguez Córdón por su involucración en este proyecto y el ánimo
recibido en todo momento.

A mi familia, por no dejarme desistir en ningún momento

A todos gracias

Índice

Índice	2
1. MEMORIA	6
1.1. Objeto	7
1.2. Antecedentes	8
1.2.1. Datos de la entidad	8
1.2.2. Localización	10
1.2.3. Organigrama.....	11
1.2.4. Productos y servicios	12
1.2.5. Modelo de Negocios	17
1.2.6. Políticas y procedimientos de la entidad	18
1.2.6.1. Entorno de Trabajo	18
1.3. Descripción Situación actual	20
1.3.1. Servidores	20
1.3.2. Redes	26
1.3.2.1. Anillo Metropolitano.....	27
1.3.2.2. VPN (Red Privada Virtual)	33
1.4. Normas y referencias	36
1.4.1. Disposiciones legales y normas aplicadas.....	36
1.4.2. Programas utilizados	36
1.4.3. Bibliografía	37
1.5. Definiciones y abreviaturas	39
1.6. Requisitos Iniciales.....	40
1.7. Alcance del proyecto	42
1.8. Estudios de alternativas y viabilidad	43

1.8.1.	Estudio de Software a utilizar	43
1.8.1.1.	Alternativa 1 administrador	43
1.8.1.2.	Alternativa 2 administrador	44
1.8.1.3.	Alternativa 3 administrador	45
1.8.1.4.	Alternativa Solución administrador	46
1.8.2.	Estudio Monitorización de equipos	47
1.9.	Descripción de la Solución propuesta	50
1.9.1.	Elementos a monitorizar	50
1.9.2.	Plantillas de equipos y especificación	52
1.9.3.	Escala de valores de incidencias	58
1.9.4.	Acciones del sistema	58
1.9.5.	Administración usuarios y tipos de medio	59
1.9.6.	Diseño de mapas interactivos	60
1.10.	Planificación temporal	64
1.11.	Resumen del presupuesto	66
2.	ANEXOS	70
A.1	ANEXO 1: Instalación de ZABBIX 3.0.....	70
A.2	ANEXO 2: Instalación de agente ZABBIX en Windows	79
A.3	ANEXO 3: instalación de agente ZABBIX en Debian / Ubuntu.....	80
A.4	ANEXO 4: Configuración de SNMP en equipos Windows.....	81
A.5	ANEXO 5: Conexión modem NOKIA TM-1.....	85
A.6	ANEXO 6: Activación SNMP FORTIGATE 800C	88
A.7	ANEXO 7: Activación SNMP HP-5500	89
A.8	ANEXO 8: Configuración de Plantilla en ZABBIX.....	91
A.9	ANEXO 9: Configuración de tipos de medios ZABBIX.....	97

A.9.1 E-mail configuración	97
A.9.2. Jabber configuración	99
A9.3. SMS Configuración.....	101
3. ESPECIFICACIONES DEL SISTEMA	106
3.1. Introducción.....	106
3.2. Objetivos.....	106
3.3. Requisitos.....	109
3.4. Matriz de Rastreabilidad Objetivos / Requisitos.....	112
4. PRESUPUESTO	116
4.1. Introducción.....	116
4.2. Presupuesto detallado	116
4.3. Presupuesto Global	117

Indice de Figuras
Figura 1: Sede Central Epicsa.....	9
Figura 2: Mapa provincia de Cádiz.....	10
Figura 3: Ubicación dentro del término municipal	10
Figura 4: Organigrama de Epicsa.....	11
Figura 5: Centro de Proceso de datos EPICSA	23
Figura 6: Servidor Dell T430.....	25
Figura 7: Red Provincial de telecomunicaciones	26
Figura 8: Diseño Jerárquico Cisco.....	27
Figura 9: Núcleo Colapsado	28
Figura 11: Rack Edificio Roma	31
Figura 13: Acceso a internet Anillo.....	33
Figura 14: FORTIGATE 800c	33
Figura 15: Router Cisco 877 k9.....	34
Figura 16: Sede externa al anillo.....	35
Figura 17: Mapa provincia de Cádiz con centros	42
Figura 18: ZABBIX agente activo.....	48
Figura 19: ZABBIX agente pasivo	49
Figura 20: Monitores Windows	53
Figura 21: Iniciadores Windows	53
Figura 22: Monitores Linux.....	54
Figura 23: Iniciadores Linux	54
Figura 24: Monitores HP.....	55
Figura 25: Iniciadores HP.....	55
Figura 26: Monitor Apache	55
Figura 27: Iniciador Apache.....	56
Figura 28: Monitor Apache 2410.....	56
Figura 29: Iniciador Apache 2410	56
Figura 23: Monitor DSMCAD.....	57
Figura 31: Iniciador DSMCAD.....	57
Figura 32: Monitor POOL OFFICE	57
Figura 33: Iniciador POOL OFFICE	57
Figura 34: Mapa de inicio en la aplicación.....	60
Figura 35: Mapa de grupos CPD	61
Figura 36: Incidencia de Windows producción.....	62

Figura 37: Mapa Anillo Metropolitano.....	62
Figura 38: Mapa provincial nodos.....	63
Figura 39: Mapa Ayto. Bornos.....	64
Figura 40: Diagrama de Gantt.....	65
Figura 41: Proceso de instalación Mysql.....	72
Figura 42: Pantalla bienvenida de Zabbix.....	75
Figura 43: Pantalla de prerequisites.....	75
Figura 44: Pantalla de conexión base de datos.....	76
Figura 45: Pantalla de detalles del servidor.....	76
Figura 46: Pantalla de preinstalación.....	77
Figura 47: Pantalla de instalación.....	77
Figura 48: Inicio de sesión.....	78
Figura 49: Activar SNMP característica.....	81
Figura 50: Propiedades de servicio SNMP Capturas.....	82
Figura 51: Propiedades de servicio SNMP Seguridad.....	83
Figura 52: Propiedades de servicio SNMP Agente.....	83
Figura 53: Puertos activos tty.....	85
Figura 54: Minicom puerta serial.....	86
Figura 55: Minicom parametros.....	86
Figura 56: Minicom salvar dfl.....	87
Figura 57: Fortigate Datos Comunidad.....	88
Figura 58: Añadir Regla Acl HP5500.....	89
Figura 59: Crear ACL HP5500.....	89
Figura 60: Comunidad HP5500.....	90
Figura 61: Activa SNMP HP5500.....	90
Figura 62: Crear plantilla zabbix.....	91
Figura 63: Creación Monitor Agente ZABBIX.....	92
Figura 64: Creación de Monitor Comprobación sencilla.....	92
Figura 65: Creación de Monitor SNMP.....	93
Figura 66; Árbol de estructura MIB General.....	94
Figura 67: Intervalos de un Monitor.....	94
Figura 68: Periodo de almacenamiento del Monitor.....	95
Figura 69: Creación de iniciador.....	96
Figura 70: Crear medio Email.....	97
Figura 71: Medio de usuario.....	98
Figura 72: Especificación de medio Email.....	98

Figura 73: Operaciones con email	99
Figura 74: Crear medio jabber	99
Figura 75: Alta de Jabber en ususrio	100
Figura 76: Asignación usuario Jabber	100
Figura 77: Asignación de operaciones al usuario jabber.....	101
Figura 78: Crear medio sms	102
Figura 79: Alta de sms en usuario.....	102
Figura 80: Asignación de teléfono al usuario.....	103
Figura 81: Asignación de operación para usuario sms	103

Indice de Tablas	
Tabla 1 : Equipos con Sistemas Operativos	22
Tabla 2: Comparativa Software Monitorización	46
Tabla 3: Equipos a Monitorizar	50
Tabla 4: Elementos a Monitorizar.....	52
Tabla 5: Resumen de Presupuesto	66
Tabla 6: Objetivo 1	106
Tabla 7: Objetivo 2	106
Tabla 8: Objetivo 3	106
Tabla 10: Objetivo 5	107
Tabla 11: Objetivo 6	107
Tabla 12: Objetivo 7	108
Tabla 13: Objetivo 8	108
Tabla 14: Objetivo 9	108
Tabla 15: Requisito 1	109
Tabla 16: Requisito 2	109
Tabla 17: Requisito 3	109
Tabla 18: Requisito 4	109
Tabla 19: Requisito 5	110
Tabla 20: Requisito 6	110
Tabla 21: Requisito 7	110
Tabla 22: Requisito 8	110
Tabla 23: Requisito 9	111
Tabla 24: Requisito 10	111
Tabla 25: Requisito 11	111
Tabla 26: Requisito 12	111
Tabla 27: Requisito 13	112
Tabla 27: Matriz de rastreabilidad.....	112
Tabla 28: Presupuesto Blade.....	116
Tabla 29: presupuesto Telefonía.....	116
Tabla 30: Presupuesto software	117
Tabla 31: Presupuesto Personal	117
Tabla 32: Resumen de Presupuesto	117

PROYECTO DE MONITORIZACIÓN DE LA GESTION DE
SISTEMAS Y REDES DE LA EXCELENTÍSIMA DIPUTACIÓN
PROVINCIAL DE CÁDIZ

CÓDIGO: IT5698929

CAPÍTULO 1: MEMORIA

DATOS CLIENTE

EMPRESA PROVINCIAL DE LA INFORMACION DE
CÁDIZ S.A

PLAZA MADRID S/N., EDIFICIO CARRANZA, FONDO
SUR, LOCAL 10,
C.P. 11010 CÁDIZ.

956 26 15 00

DATOS AUTOR

BRAULIO PAREJA MANZANARES

INGENIERO INFORMÁTICO

VIRGEN 5, CONIL, CADIZ
C.P. 11140

BRAULIO.PAREJA.MANZANARES@DIPUCADIZ.ES

FECHA DE PRESENTACIÓN

JULIO 2017

FIRMA:

DURACION
ESTIMADA

600 HORAS

BRAULIO PAREJA MANZANARES

1. MEMORIA

La empresa pública EPICSA (Empresa Provincial de Información de Cádiz, Sociedad Anónima) proporciona servicios técnicos de Tecnología de la Información y Comunicaciones (en adelante TIC) a la Excma. Diputación Provincial de Cádiz, a los organismos dependientes de ésta, así como también a los distintos ayuntamientos de la provincia. Entre estos servicios TIC, podemos destacar la infraestructura de red dedicada, el alojamiento de webs y aplicaciones, bases de datos, servicios webs, correo electrónico, administración electrónica, etc., siendo su intención seguir prestándolos y aumentarlos.

Actualmente, para poder ofrecer un buen servicio se necesita monitorizar los servicios prestados, ya que un servicio parado un tiempo prolongado puede causar pérdidas a la empresa. Los objetivos de una infraestructura de monitorización de sistemas informáticos son principalmente la prevención de incidencias y conocer el aprovechamiento de los recursos disponibles. Toda organización debería contar con su propio sistema de monitorización, pues éstos objetivos son importantes en cualquier entidad independientemente de su tamaño.

El monitoreo, a rasgos generales, consiste en la observación del curso de uno o más parámetros para detectar anomalías eventuales. Al igual que un vigilante de seguridad descubre algún movimiento extraño (como el ingreso de un individuo no identificado en el edificio que vigila), en el ámbito de la administración de redes, se conoce con el nombre de monitoreo de red a un sistema que realiza un control constante de una red de ordenadores, intentando detectar defectos y anomalías; en caso de encontrar algún desperfecto, envía un informe a los administradores e incluso podría llegar a tomar una decisión para que no sea necesaria la actuación de un administrador.

Para llevar a cabo el proyecto tendremos que tomar decisiones tales como: qué monitorizar, cómo monitorizar, cuándo alertar y qué herramienta utilizar. Al encontrar gran variedad de aplicaciones en el mercado, debemos decidir qué herramienta sería más eficiente para la Empresa Provincial de Información de Cádiz, Sociedad Anónima.

1.1. Objeto

El objetivo de éste proyecto es dotar a EPICSA de un sistema de monitorización, actualmente ausente, para así poder centralizar todos los eventos que ocurren en los servicios prestados. Puesto que la empresa sigue creciendo y prestando más servicios, es necesario que el departamento de Sistemas y Redes esté informado de todo lo que ocurre en la red, así como el seguimiento de los servidores en un periodo prolongado, por si se tuviera que tomar alguna decisión sobre algún equipo.

Para cubrir la necesidad que precisa la empresa, buscaremos o crearemos una aplicación para poder llegar al objetivo de monitorizar todo el sistema que dependa de ella; y a su vez, poder estar notificados en cada momento de todo lo que sucede, no sólo de tenerlo registrado, sino que en el momento que suceda algo significativo, estemos alertado. Y además, en la medida de lo posible, que dicho programa sea capaz de tomar alguna decisión para poder restablecer los servicios.

1.2. Antecedentes

La Excma. Diputación Provincial de Cádiz, tiene delegada sus funciones y servicios de tecnología de la información y comunicación en la empresa pública EPICSA, la cual le gestiona, asesora, proporciona y mantiene todos los servicios informáticos, tanto internos de la propia corporación, como los externos (orientados a la ciudadanía), así como también, a los ayuntamientos y administraciones locales más pequeñas.

Actualmente, se cuenta con un gran número de servicios a disposición de los ciudadanos y de la propia corporación, por lo cual ya no sólo basta con los técnicos y administradores para cubrir los servicios ofrecidos, sino que se tienen que plantear algún método para poder tener centralizado y localizado todos los servicios que son ofrecidos por dicha empresa, pues éstos deben de estar cubiertos 24 horas 365 días al año.

En la actualidad, se tiene conocimiento de los servicios que están caídos cuando los usuarios van a hacer uso de ello, por tanto existe la necesidad de anteponernos a que el usuario nos diga que el servicio no se encuentra en funcionamiento. Aun disponiendo de alertas algunos dispositivos, se requiere centralizar todo.

1.2.1. Datos de la entidad

EPICSA, Empresa Provincial de Información de Cádiz S.A. es una empresa creada en 1984 por la diputación de Cádiz, con el objetivo de dar asistencia técnica informática integral, formación, comercialización y desarrollo e implementación de aplicaciones informáticas, tanto de la propia Diputación como a sus organismos, empresas y municipios de menos de 20000 habitantes.

En este contexto, las tecnologías de la información son consideradas como herramientas con un enorme potencial para configurar estructuras organizativas y modelos de gestión de los servicios que ofrezcan una respuesta única, ágil, eficiente, de calidad y transparente a los ciudadanos.

De ésta manera, las tecnologías de información podrían ser un motor de cambio para las organizaciones, entendiendo como tal no sólo la modificación de los elementos técnicos sino también, lo que es más importante: el cambio en los valores y comportamientos que configuran la cultura organizativa existente, evidenciando la necesidad de articular políticas, procedimientos y servicios

integrados y transversales que respondan con coherencia a las necesidades de los ciudadanos.

EPICSA centra su actividad en garantizar el funcionamiento de las redes de datos y de las aplicaciones corporativas, en el ámbito que le es de su competencia a nivel provincial, para lo cual estamos desarrollando acciones para la adaptación de nuestros servicios a estas actividades.

En la tarea del desarrollo de la e-Administración es en la que estamos inmersos ya que, en la actualidad, EPICSA ejecuta las directrices de las políticas relativas al ámbito del desarrollo y la generalización de las tecnologías de la información de la Diputación a través del Área de Presidencia y Coordinación y en relación a las líneas maestras que está diseñando la Junta de Andalucía para toda la comunidad autónoma.



Figura 1: Sede Central Epicsa¹

¹ «EPICSA».

1.2.2. Localización

Actualmente EPICSA se encuentra localizada en la capital de la provincia Gaditana, Plaza Madrid s/n., Edificio Carranza, Fondo Sur, Local 10, Código Postal 11010 Cádiz.

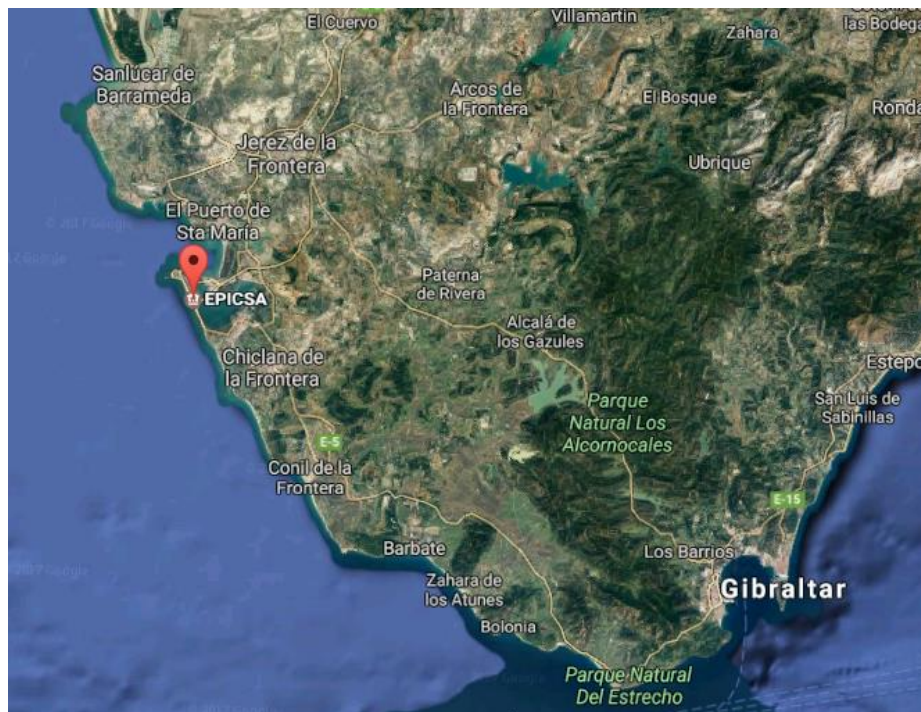


Figura 2: Mapa provincia de Cádiz

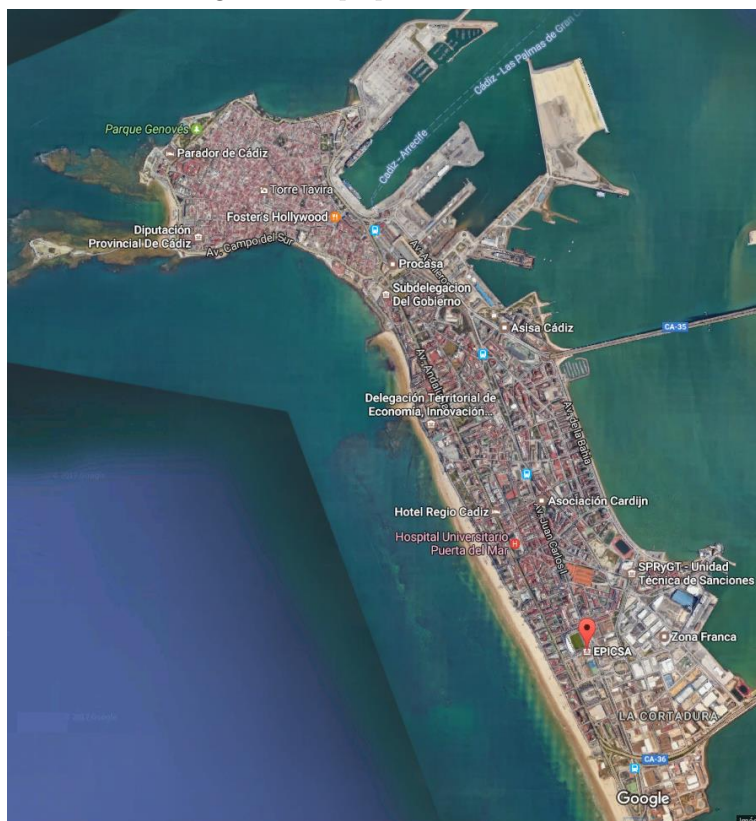


Figura 3: Ubicación dentro del término municipal

1.2.3. Organigrama

EPICSA se encuentra distribuida con los siguientes departamentos:



Figura 4: Organigrama de Epicsa

Gerencia: Aquí se encuentra el Gerente de la Empresa Pública de Información de Cádiz, Sociedad Anónima. Responsable en última instancia de la misma y es quien toma las decisiones importantes de la empresa.

Dirección Técnica: Este departamento es unipersonal, formado por el Director Técnico de la misma, siendo la persona encargada de tomar las decisiones técnicas y la línea que emprenderá la empresa en cuestiones técnicas.

Administración: Personal encargado de labores administrativas.

Gestión Corporativa: Este es el departamento más voluminoso en cuanto a personal humano de la empresa. En él se encuentra el conjunto de programadores y analistas del software corporativo

Gestión Municipal y Web: Este es otro departamento correspondiente al Área de Gestión en el cual se encuentran los programadores y analistas correspondientes al software relativo a los municipios, así como las Webs Municipales de estos.

Departamento de Comunicación e Innovación: Departamento en el cual se concentra la comunicación y relaciones con los medios, así como la investigación de nuevos productos y software para poder incorporarlos al catálogo de productos.

Sistemas y Redes: Este departamento se encarga de la gestión de las redes tanto corporativas como municipales, así como de la gestión y mantenimiento de los servidores de toda la corporación. También se encuentra como un subdepartamento el departamento de explotación y Centro de Atención al Usuario, el cual es el encargado de atender, registrar y solucionar las incidencias de primer nivel de los usuarios, así como de las incidencias y sugerencias de la ciudadanía.

En este último departamento es en el cual nos vamos a centrar, ya que es el departamento encargado del mantenimiento de la infraestructura que ha construido EPICSA.

1.2.4. Productos y servicios

EPICSA ofrece un amplio catálogo de servicios y productos destinados a atender las necesidades de gestión de la Diputación Provincial, sus organismos y entidades dependientes, así como las de los ayuntamientos de la provincia.

A modo de listado reflejamos los principales productos con los que cuenta:

Contrat@. Gestión de compras y contratación.

Gestión de procedimientos de contratación de obras, suministros y servicios de la Diputación de Cádiz y sus organismos autónomos.

Contabilidad.

Gestión de la contabilidad de la entidad corporativa, así como de los ayuntamientos y entidades asociadas.

Control de Presencia. Gestión de asistencia de empleados y control de vacaciones.

Gestión de asistencia de empleados en función de sus jornadas asignadas y control de vacaciones y festivos particularizada a las distintas condiciones laborales.

Convocatoria Electrónica de Órganos Colegiados

Permite convocar nominativamente a los integrantes de los diversos órganos colegiados de la corporación por medios electrónico.

Decretos

La aplicación gestiona de manera telemática e integral la tramitación de Decretos, Notificaciones, Traslados, Certificados y la documentación relacionada, así como de la elaboración y remisión de extractos, y la composición automática del libro de Decretos

Decret@

Gestión de decretos, similar a la anterior pero personalizada para los distintos ayuntamientos de la provincia.

Desarrollos Webs

Con el objetivo de facilitar a los ayuntamientos, entidades locales e instituciones públicas su presencia en internet, EPICSA desarrolla portales web a medida, incluyendo el diseño, hospedaje y la gestión de dominios. Para ello, emplea siempre la última tecnología con los más potentes gestores de contenidos que ofrece actualmente el mercado. Entre las webs municipales podemos destacar las siguientes:

Ayuntamientos

Alcalá de los Gazules (<http://www.alcaladelosgazules.es>)

Alcalá del Valle (<http://www.alcaladelvalle.es>)

Algar (<http://www.algar.es>)

Algodonales (<http://www.algodonales.es>)

Barbate (<http://www.barbate.es>)

Benalup-Casas Viejas (<http://www.benalupcasasviejas.es>)

Benaocaz (<http://www.benaocaz.es>)

Bornos (<http://www.bornos.es>)

Castellar de la Frontera (<http://www.castelladelafrontera.es>)

Conil de la Frontera (<http://www.conildelafrontera.es>)

El Bosque (<http://www.ayto-elbosque.es>)

El Gastor (<http://www.elgastor.es>)

Espera (<http://www.espera.es>)

Grazalema (<http://www.grazalema.es>)
Jimena de la Frontera (<http://www.jimenadelafrontera.es>)
Olvera (<http://www.olvera.es>)
Paterna de Rivera (<http://www.paternaderivera.es>)
Prado del Rey (<http://www.pradodelrey.es>)
Puerto Serrano (<http://www.puertoserrano.es>)
San José del Valle (<http://www.sanjosedelvalle.es>)
Setenil de las Bodegas (<http://www.setenildelasbodegas.es>)
Torrealháquime (<http://www.torrealhaquime.es>)
Vejer de la Frontera (<http://www.vejerdelafrontera.es>)
Villaluenga del Rosario (<http://www.villaluengadelrosario.es>)
Villamartín (<http://www.villamartin.es>)
Zahara de la Sierra (<http://www.zaharadelasierra.es>)

Entidades Locales (ELA)

Coto de Bornos (<http://www.cotodebornos.es>)
El Santiscal (<http://www.elsantiscal.es>)
El Torno (<http://www.eltorno.es>)
Estella del Marqués (<http://www.estelladelmarques.es>)
Facinas (<http://www.facinas.es>)
Guadalcacín (<http://www.guadalcacin.es>)
Jédula (<http://www.jedula.es>)
La barca de la Florida (<http://www.labarcadelaflorida.es>)
San José de Malcocinado (<http://www.malcocinado-badalejos.es>)
Nueva Jarilla (<http://www.nuevajarilla.es>)
San Martín del Tesorillo (<http://www.sanmartindeltesorillo.es>)
San Isidro del Guadalete (<http://www.sanisidrodelguadalete.es>)
Tahivilla (<http://www.tahivilla.es>)
Torrecera (<http://www.torrecera.es>)

Diagnósticos. Sistema de Gestión de Pruebas Diagnósticas.

Gestión de pruebas diagnósticas a pacientes con dependencias.

Digitalización certificada. Digitalización y firma de documentos electrónicos. Se digitaliza mediante el escaneado de documentos en papel y se procede a la firma de los mismos certificando que la copia es fiel a su original.

eCO. Comunicaciones Interiores y Oficinos.

El sistema de Comunicaciones Interiores y Oficinos tiene como finalidad la gestión de comunicaciones entre organismos y otras unidades organizativas de la administración sin usar papeles.

ePadron. Gestión del padrón de habitantes

La legislación actual obliga a los ayuntamientos a gestionar el registro de los habitantes de su municipio con medios informáticos (artículo 17 de la Ley 7/1985). Esta aplicación cubre esta necesidad para los municipios dentro del ámbito de actuación de la Diputación de Cádiz, esto es, aquellos con menos de 20.000 habitantes.

eTIR. Aplicación de Gestión electrónica de Tributos, Ingresos y Recaudación.

Es la aplicación de Gestión electrónica de Tributos, Ingresos y Recaudación. Utilizada por el Servicio Provincial de Recaudación y Gestión Tributaria de la Diputación Provincial.

Histórias Clínicas. Gestión de historias clínicas de pacientes con dependencias. Gestión de historias clínicas, control de analíticas y emisión de recetas a pacientes con dependencias.

IDE Cádiz. Infraestructura de Datos Espaciales.

La Infraestructura de Datos Espaciales de la Provincia de Cádiz (IDECádiz) pone a disposición de los ciudadanos, empresas y administraciones la información geográfica producida por la Diputación de Cádiz.

Perfil del Contratante. Gestión de publicaciones en el perfil de contratante

Gestión de publicaciones de licitaciones realizadas por una entidad en el perfil de contratante.

Planificación e Infraestructuras. Gestión de planes de actuaciones.

Gestión, elaboración y seguimiento de planes provinciales y de otro tipo, realizados por la Diputación para control de actuaciones, tanto propias como solicitadas por los ayuntamientos.

Port@firmas

Permite la firma electrónica de documentos conforme a la actual legislación. A su vez, necesita emplear los Servicios Webs de @firma.

Registro de Licitadores.

Gestión del Registro de Licitadores para controlar la entrega de documentación, su capacidad para licitar actuaciones, así como su situación tributaria.

Sede Electrónica. Gestión de trámites electrónicos y oficina Virtual

Facilita el acceso por medios electrónicos de los ciudadanos a la información y trámites administrativos, a cualquier hora durante todos los días del año, teniendo la misma validez que si se efectúan de forma presencial.

SEM. Sedes Electrónicas Municipales.

Son las Sedes electrónicas pertenecientes a cada ayuntamiento para facilitar la gestión de trámites y la administración electrónica a la ciudadanía.

Sell@. Digitalización de documentos.

Permite la digitalización de múltiples documentos, obteniendo copias en formato electrónico de los originales en papel, firmados digitalmente y con los metadatos obligatorios establecidos por el Esquema Nacional de Interoperabilidad, así como los que se consideren de interés para su almacenamiento en el repositorio documental.

Además de estos productos, EPICSA ofrece el servicio de intranet e internet a todos los ayuntamientos adheridos a la Excma. Diputación de Cádiz, así como sus propios servidores y mantenimiento de toda la infraestructura informática, junto con el soporte a los usuarios.

1.2.5. Modelo de Negocios

EPICSA presta los siguientes servicios fundamentalmente a la Excm. Diputación Provincial de Cádiz:

- Compatibilizar todas las áreas y servicios que presta la administración, permitiendo el intercambio de datos y de información. Al mismo tiempo, conseguir un ahorro importante de recursos técnicos y humanos al permitir trabajar con aplicativos comunes y con una formación común. Como tareas básicas se acometen: unificación de equipos informáticos, aplicaciones informáticas, herramientas ofimáticas y desarrollos
- Automatización y optimización de aquellos procesos susceptibles de ser mecanizados a través de aplicaciones informáticas
- Servicios de alojamiento (en adelante, hosting), diseño, creación y mantenimiento de diversas páginas webs que componen dicha administración así como de sus organismos y entidades dependientes
- Servicios de correo electrónico corporativo y municipales
- Servicios de asesoramiento y asistencia técnica TIC a entidades locales más pequeñas
- Servicios de redes informáticas. Instalación, gestión y configuración, tanto de redes internas de la propia administración como de los organismos y entes dependientes.
- Servicios de administración electrónica y trámites electrónicos para la ciudadanía (Ventanilla virtual, Sede Electrónica)
- Servicios de gestión corporativa. Aplicaciones de uso interno para el propio funcionamiento de la entidad y sus organismos dependientes,

así como las entidades locales(ayuntamientos y entidades locales autónomas, en adelante ELA)

- Servicios de gestión documental

Como hemos indicado anteriormente, EPICSA se ha marcado como objetivo extender sus servicios, agilizándolos y optimizándolos tanto para los actuales servicios y entidades, como para incrementar estos a la vez que proporcionar nuevos servicios y funciones para otras entidades de mayor envergadura. Para ello, está contactando con los diversos municipios a los que aún no les presta servicios para ofrecerle su carta de productos y sumarlos juntos a los demás. Su objetivo final pretende ser la nube de servicios de administración electrónica de la provincia para así agilizar y ofrecer servicios de calidad, robustez y fiabilidad a la ciudadanía de forma homogénea, accesible e intuitiva. Estos servicios podrán ser ofrecidos de diversa manera:

- A través de servicios software: En el cual se ofrece un determinado software independientemente de los servidores o máquinas que este necesite.
- A través de servicios de computación: En el cual se ofrecen máquinas de computación, servidores, en el cual los usuarios se auto gestionan. En este caso EPICSA “sólo” se encargará de mantener a dichas máquinas.

1.2.6. Políticas y procedimientos de la entidad

En este apartado vamos a destacar el entorno de trabajo que utiliza EPICSA para la preparación de los equipos que van a suministrar los servicios. Vamos a proporcionar los entornos con los que actualmente cuenta la empresa.

1.2.6.1. Entorno de Trabajo

En EPICSA podemos distinguir entre 3 entornos de trabajo:

Desarrollo

Este entorno se emplea para albergar el software que los compañeros de Gestión se encuentran diseñando y programando en base a las necesidades de la

corporación, de los ayuntamientos u organismos dependientes. Las máquinas empleadas para este propósito cuenta con recursos más limitados ya que su empleo, como hemos mencionado, solo es para un grupo reducido de personas (programadores, diseñadores y analistas principalmente) que no requieren de tantos recursos, así como la disponibilidad de las mismas que sólo serán requeridas durante el horario laboral de las mismas. La cantidad de datos que albergan y se usan también serán muy reducidos puesto que se tratan solamente de datos básicos para validar y verificar su funcionamiento.

Preproducción

Este entorno se emplea para albergar el software una vez diseñado y probado por el equipo de desarrollo y que está disponible para la realización de pruebas de verificación y validación por los usuarios finales de la corporación. Este entorno albergará una cantidad mayor de datos ya que serán los propios usuarios finales de la aplicación quien los nutrirán y emplearán para entender y conocer el sistema, así como una verificación y validación final del mismo.

Producción

Este entorno se emplea para las máquinas en producción, es decir, para nuestro entorno final de uso y explotación del mismo, ya sea personal propio de la corporación y organismos dependientes como a la ciudadanía. La cantidad de datos a emplear será mayor que en los entornos anteriores y adecuados al servicio que preste. Los recursos para estas máquinas han de ser mayores, así como su fiabilidad y estabilidad del mismo.

1.3. Descripción Situación actual

EPICSA centra su actividad en garantizar el funcionamiento de las redes de datos y de las aplicaciones corporativas en el ámbito de su competencia a nivel provincial, para lo cual desarrolla acciones para la adaptación de nuestros servicios a estas actividades.

En la sede de la empresa podemos encontrarnos con el CPD en la cual están corriendo todos los servicios y productos ofrecidos, y la centralización de las redes siendo éste un punto principal de conexión con los distintos ayuntamientos de la provincia, y una de las salidas a internet que tiene la diputación de Cádiz.

1.3.1. Servidores

En cuanto a servidores del CPD, EPICSA maneja y gestiona distintas versiones de sistemas operativos. Según el sistema operativo podemos encontrarnos con los distintos servidores que gestionan actualmente EPICSA Windows, IBM, Linux, Solaris.

Windows.

Microsoft Windows 2000 server. Actualmente cuenta con 2 servidores licenciados destinados principalmente para un software antiguo y que no es posible ejecutar en versiones superiores a este, el cual permite la conexión entre este y servidores IBM S/390.

Microsoft Windows 2003 Server R2.

2 servidores destinados a servidores webs mediante Microsoft Internet Information Servers (IIS) para servir contenido en asp, asp.net, html, etc.

1 servidor controlador de impresión.

5 servidores para alojar servidores de aplicaciones mediante servicios de Citrix (XenApp).

2 servidores para alojar Microsoft Exchange Server para gestionar los buzones y cuentas de correo electrónico de la Diputación y de los distintos ayuntamientos de la provincia.

2 Servidores (uno desarrollo y otro producción) para alojar servidores con base de datos Microsoft SQLServer.

Microsoft Windows 2008 Server.

4 servidores en su CPD destinados a contener los servicios de controladores de dominio (Active Directory), los cuales a su vez ofrecen servicios de DNS a los distintos equipos que conforman la red corporativa de la Diputación de Cádiz y sus organismos autónomos.

25 servidores como controles de dominio, uno por cada ayuntamiento o ELA a los cuales presta servicios (estos no se encuentran alojados en las instalaciones de Epicsa sino en cada ayuntamiento).

1 servidor para alojar el servidor de gestión de copias de seguridad IBM Tivoli.

2 Servidores para el clúster de datos (unidades en red donde los usuarios guardan sus datos corporativos)

Linux.Suse Linux Enterprise Server.

Epicsa cuenta con 82 servidores de esta distribución de Linux con diferentes versiones del mismo (desde la versión 9 a la versión 11). Principalmente emplea estos servidores como servidores de aplicaciones webs y contenedores servlets, así como servidores de php y base de datos relacionales como MySQL o PostgreSQL.

CentOS.

En esta distribución de Linux también se emplea para servidores y contenedores servlets de Java.

Ubuntu Server.

Esta distribución menos usada en Epicsa, contiene principalmente la aplicación de GIS (IDE Cádiz), con base de datos PostgreSQL y postgis como integración.

IBM.

Cuenta con un servidor IBM AS400 el cual está próximo a desaparecer debido al cambio y migración de la aplicación de recaudación desde este sistema a un sistema Java/Oracle.

Servidor IBM S/390. Servidor para aplicaciones de la nómina de Diputación y sus organismos, así como para el control horario del personal de la misma.

Resumiremos todos los equipos anteriores citados en una tabla para poder visualizarlo más rápidamente

TIPO	Sistema Operativo	Uso	Cantidad
Windows	2000 Server	Enlace con IBM S/390	2
Windows	2003 Server	Servidor Web	2
Windows	2003 Server	Controlador Impresión	1
Windows	2003 Server	Servicio Citrix	5
Windows	2003 Server	Exchange Server	2
Windows	2003 Server	BD Microsoft SQLServer	2
Windows	2008 Server	Controlador de dominio	4
Windows	2008 Server	Gestor de copias	1
Windows	2008 Server	Clúster de datos	2
Windows	2008 Server	Domino de Ayuntamientos	25
Linux	Suse Linux Enterprise Server (v9-11)	Aplicaciones Web	82
Linux	Cent OS	Aplicaciones Web	10
Linux	Ubuntu Server	Aplicaciones de Gestión y Monitorización	4
IBM	AS400	Aplicación Recaudación	1
IBM	S390	Nominas	1

Tabla 1: Equipos con Sistemas Operativos

Ahora mostramos el CPD donde se encuentra alojados los servidores físicos de EPICSA en los que tenemos los distintos servidores indicados anteriormente independientemente de que sean de producción, preproducción o desarrollo.



Figura 5: Centro de Proceso de datos EPICSA

Podemos decir que contamos con sistemas de virtualización y máquinas físicas, pero en nuestro proyecto va a ser independiente de cómo sea la máquina, si física o virtual, porque la vamos a monitorizar a través del sistema operativo que dispongan, siempre que hablemos de los servidores.

Vamos a indicar con qué equipamiento de virtualización dispone EPICSA actualmente en sus instalaciones de procesamiento de datos, el software de virtualización es VMWare vSphere 5.1 contando con 3 clúster y más de 100 máquinas virtuales:

- **Clúster Desarrollo** formado por 3 equipos físicos correspondientes a un blade IBM HS21 destinado a las máquinas de desarrollo. Cuenta con licencia VMWare Estándar:
 - Características:
 - Intel Xeon E5504 @ 2GHz (2 Sockets quad-core)
 - 16 Gb RAM
 - 1 Discos duros 60 GB
 - Conectadas a la cabina de discos de Epicsa, en la cual mediante datastores almacenan todas las máquinas virtuales para así formar el clúster.
 - Actualmente cuenta con 37 máquinas Virtuales
- **Clúster Producción 1** formado por 6 equipos físicos correspondientes a un blade IBM HS22 destinado a las máquinas de producción. Cuenta con licencia VMWare Enterprise Plus
 - Características:
 - 2 sockets quad-core Intel Xeon E5540 @2.53GHz
 - 24 GB de RAM
 - 1 Disco duro de 60 GB
 - Conectadas a la cabina de discos de Epicsa, en la cual mediante datastores almacenan todas las máquinas virtuales para así formar el clúster.
 - Actualmente cuenta con 42 máquinas Virtuales
- **Clúster Producción 2** formado por 2 equipos físicos correspondientes a un IBM 3850 M2 destinado a las máquinas de producción. Cuenta con licencia VMWare Enterprise Plus
 - Características:
 - 4 sockets 6-core Intel Xeon X7460 @2.66GHz
 - 128 GB de RAM
 - 1 Disco duro de 60 GB
 - Conectadas a la cabina de discos de Epicsa, en la cual mediante datastores almacenan todas las máquinas virtuales para así formar el clúster.
 - Actualmente cuenta con 44 máquinas Virtuales

Tenemos que indicar que los servidores de los ayuntamientos no se encuentran en el CPD, ya que están alojados cada uno en su respectivo centro como máquinas físicas, utilizadas como controlador de dominio y almacenamiento de datos de los usuarios y a su vez, ofrece servicio de DNS para los usuarios de la red corporativa de cada ayuntamiento, contando con el siguiente modelo de servidor ya que se está realizando el cambio de servidores en todos los ayuntamientos adheridos a la diputación de Cádiz

- **Dell T430**

- Características:

- 2 sockets 6-cores Intel Xeon E5 2609 v4 @2.4GHZ
 - 16 GB RAM
 - 4 TB de Disco (Esta capacidad es el total de los discos que lleva ya que tienen raid en espejo por lo que contraria con una capacidad de 2TB)
 - Fuente Remplazo en caliente



Figura 6: Servidor Dell T430

1.3.2. Redes

En este apartado, vamos a diferenciar entre 2 tipos de infraestructura que emplea EPICSA para interconectar los distintos Ayuntamientos con los servicios ofrecidos y la red utilizada por la Excma. Diputación de Cádiz, ya que cuenta con varias sedes y organismos repartidos por distintos lugares de la ciudad, como en distintas poblaciones de la provincia gaditana.

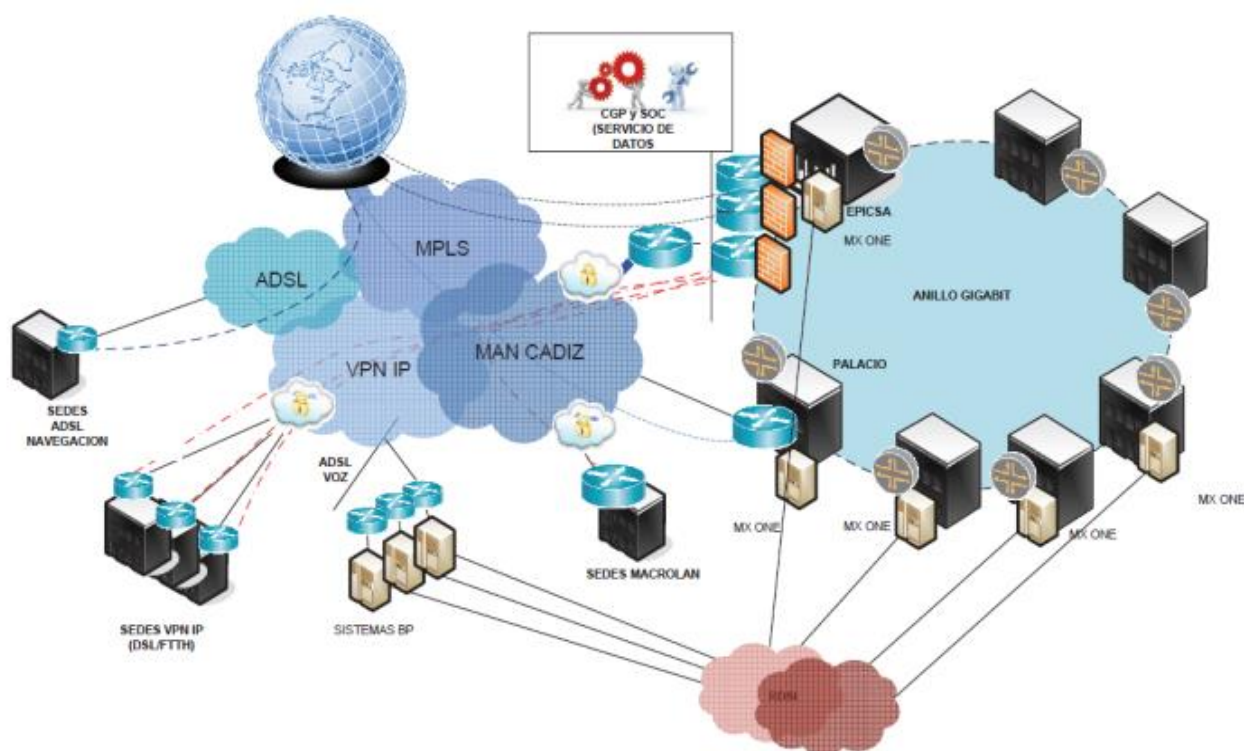


Figura 7: Red Provincial de telecomunicaciones

Tenemos que indicar que EPICSA es el principal centro de intercomunicaciones, pues tanto las sedes de diputación y los distintos órganos de gobierno de la provincia de Cádiz están conectados a esta sede central, para así poder distribuir sus productos y servicios.

1.3.2.1. Anillo Metropolitano

Primeramente, vamos a indicar que el anillo está compuesto por una red jerárquica en la que todos los nodos del anillo actúan como núcleo colapsado, qué queremos decir con esto, pues que los conmutadores que hacen de núcleo también lo hacen de distribución y además tenemos los conmutadores de acceso. Vamos a explicar en qué se compone una red jerárquica.

El diseño de una red jerárquica implica la división de la red en capas independientes. Cada capa cumple funciones específicas que definen su rol dentro de la red general. El modelo de diseño jerárquico típico se separa en tres capas: capa de acceso, capa de distribución y capa de núcleo.

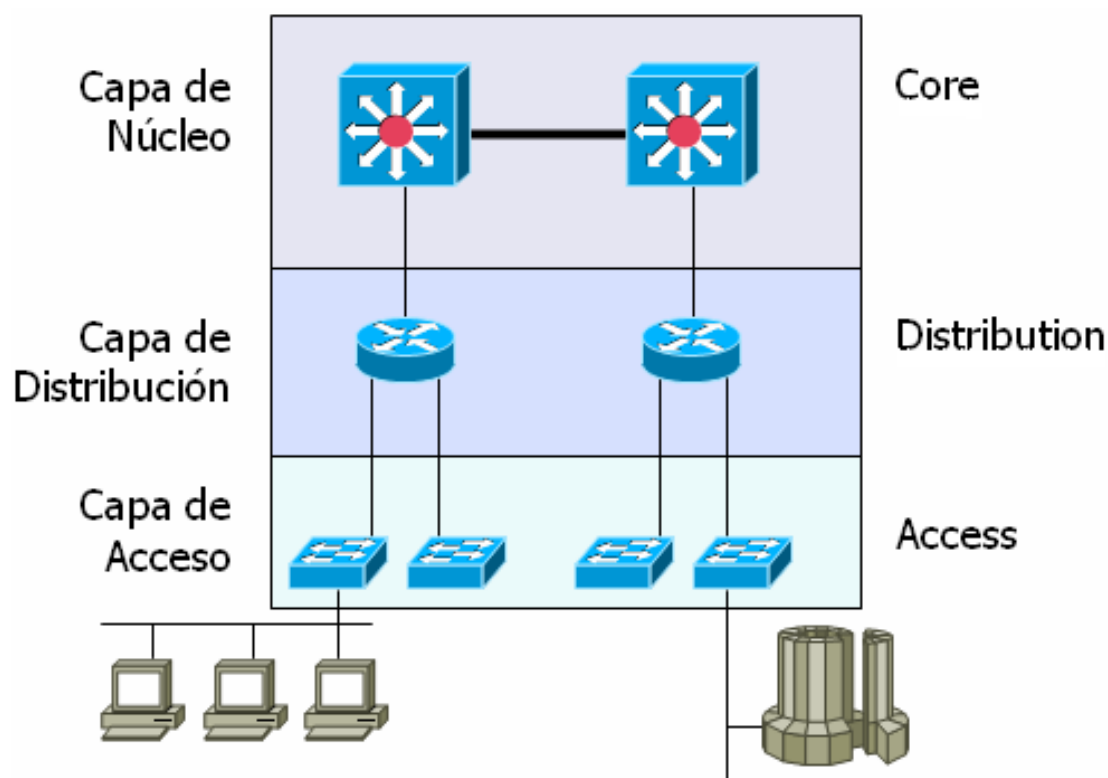


Figura 8: Diseño Jerárquico Cisco²

En las cuales sus funciones son:

- Capa de acceso:
 - El propósito principal es aportar un medio de conexión de los dispositivos a la red y controlar que dispositivos pueden comunicarse en la red. Controlando a los usuarios y el acceso a los grupos de trabajo

² «El modelo jerárquico de 3 capas de Cisco».

- Capa de distribución
 - Es el medio de comunicación entre la capa de acceso y la capa de núcleo. Las funciones de esta capa son proveer ruteo, filtrado, acceso a la red WAN y determinar que paquetes deben llegar al Core. Además, determina cuál es la manera más rápida de responder a los requerimientos de red, por ejemplo, cómo traer un archivo desde un servidor.
- Capa de Núcleo
 - es literalmente el núcleo de la red, su única función es switchear tráfico tan rápido como sea posible y se encarga de llevar grandes cantidades de tráfico de manera confiable y veloz, ya que agrega el tráfico de todos los dispositivos de distribución.³

Una vez que ya sabemos las funciones de cada capa, EPICSA trabaja con este modelo jerárquico, pero con una peculiaridad, y es que combina la capa de distribución y núcleo creando un núcleo colapsado.

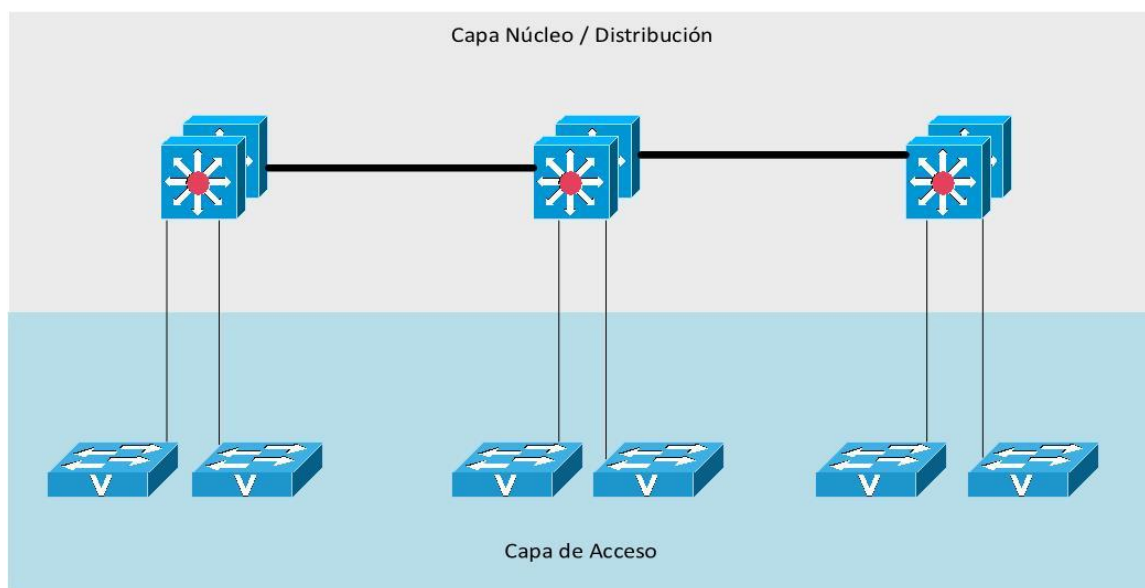


Figura 9: Núcleo Colapsado

³ «Campus_Cisco_Resumen_Diseño.pdf».

Como vemos en la figura 9 cada edificio tiene un conmutador, bueno clúster de conmutadores de la capa de núcleo colapsado y sus conmutadores de acceso. También destacar que cada sede tiene su propia Vlan identificadas por departamentos y racks cercanos.

Vamos a empezar a mostrar cómo está conectado el anillo metropolitano de la Excm. Diputación de Cádiz, para que nos hagamos una idea de lo que actualmente disponemos para poder ver qué monitorizar y ver cómo es de importante saber en cada momento que está activo o no, ya que si hay algún corte en el anillo, no nos daríamos cuenta, se cambiarían las métricas y tomaría otro camino que sería más largo pero no menos efectivo.

La distribución se puede ver a continuación. Actualmente dispone de un anillo de fibra óptica Gigabit que interconecta las distintas sedes que se ubican en la ciudad de Cádiz. Estas sedes son conectadas con clúster de conmutadores de manera que cada uno de ellos dispone de dos tarjetas LX del tipo SFP conectada, al nodo anterior y al siguiente. En algunos casos, como vemos en la figura 1º, tendremos unos ramales que nos llevarán a otras sedes, pero no están dentro del anillo que actúan como conmutadores de acceso.

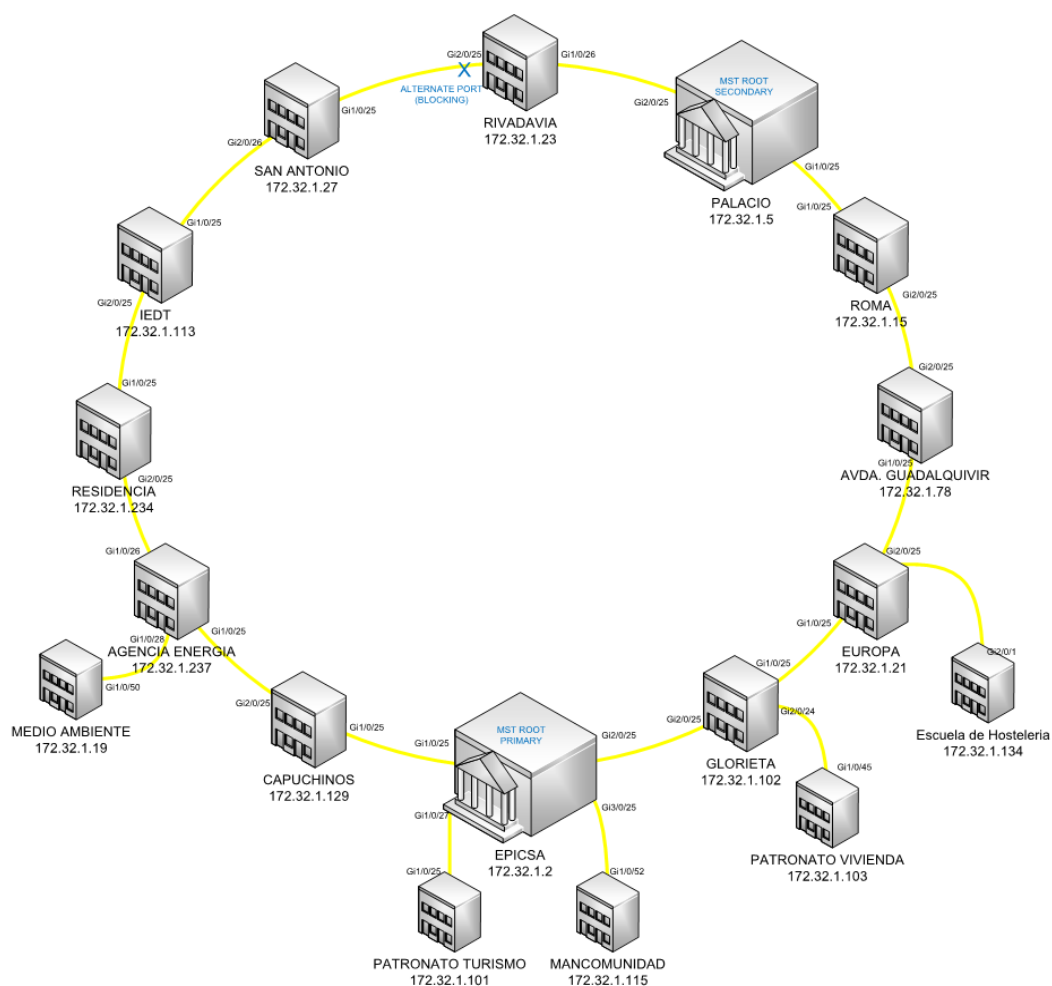


Figura 10: Anillo Metropolitano

En cada nodo del anillo contamos con un clúster de conmutadores, ofreciendo así, una mayor disponibilidad de la red. Por lo que si sufriéramos un corte los datos tomarían el sentido contrario para llegar al destino, con el clúster tendríamos disponibilidad aun con ese corte. Los conmutadores que forman el anillo son HP del modelo 5500HI series, son plataformas de 1RU con conectividad line-rate y arquitectura mono blocking ofreciendo puertos 1Gigabit Ethernet y 10 Gigabit Ethernet, con fuentes de alimentación en caliente y redundante es decir que podríamos cambiar una fuente sin que el conmutador tenga que parar. Estos conmutadores a la vez van conectados a otros de su misma sede que les dan acceso a los usuarios y con ellos poder llevar la red a los usuarios finales. Vamos a tomar como ejemplo en la figura 11 el rack principal de la sede Roma para situarnos.

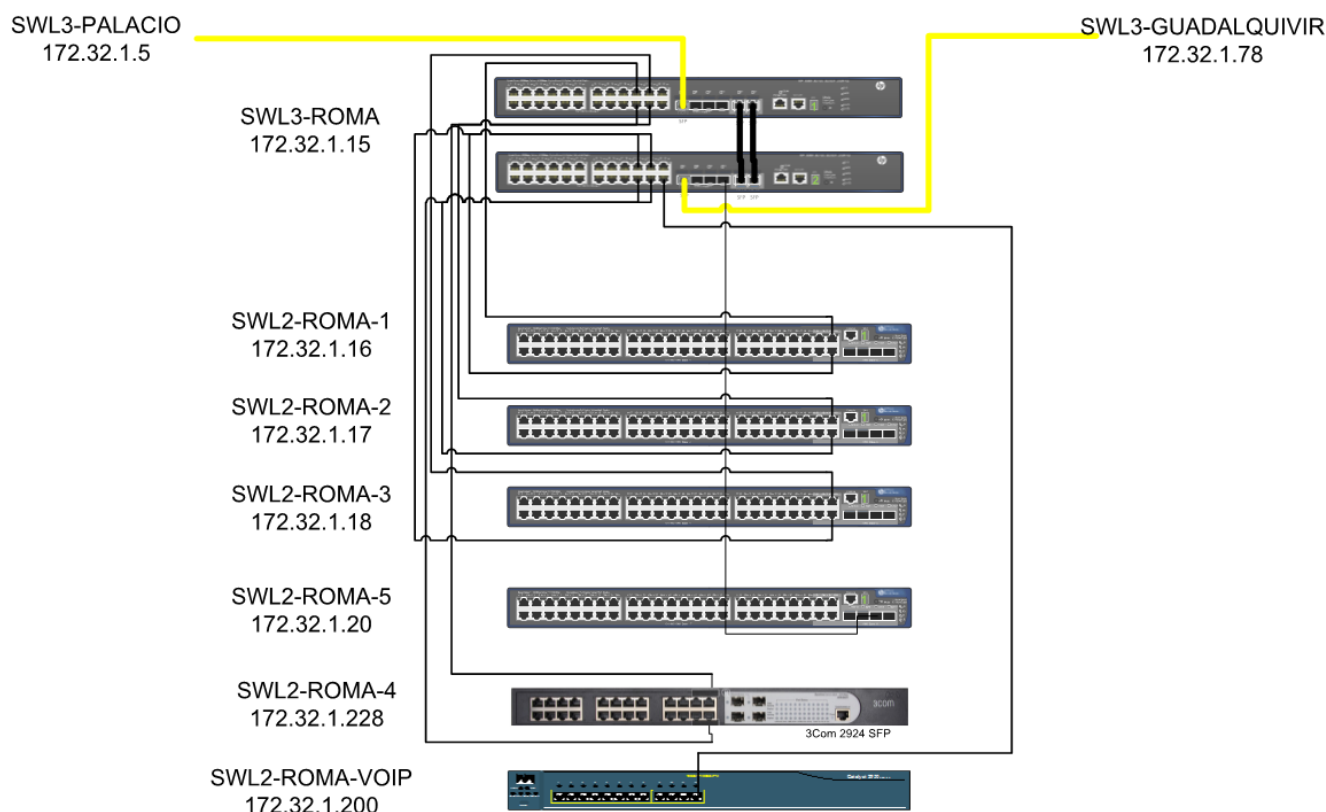


Figura 11: Rack Edificio Roma

Como muestra la imagen nos llega el enlace del conmutador de capa 3 de la sede Palacio al conmutador Maestro de capa 3 de la sede roma y continuamos el anillo por el Conmutador Esclavo de capa 3 hacia la sede Guadalquivir. Y como podemos observar cada conmutador de acceso esta interconectado con ambos conmutadores tanto Maestro como esclavo para que sea redundante y así poder tener mayor disponibilidad. Estos conmutadores de acceso cuenta con las siguientes especificaciones, es el modelo hp 5120 series, son plataformas de 1 RU con conectividad line-rate, ofreciendo puertos 1GibabEt Ethernet y 4 puertos SFP Gbe y podríamos apilar hasta una máximo de 4 dispositivos. Vamos a mostrar el núcleo de una sede cualquiera, para poder identificar mejor el clúster que forma parte del núcleo colapsado de la red jerárquica que tiene EPICSA.

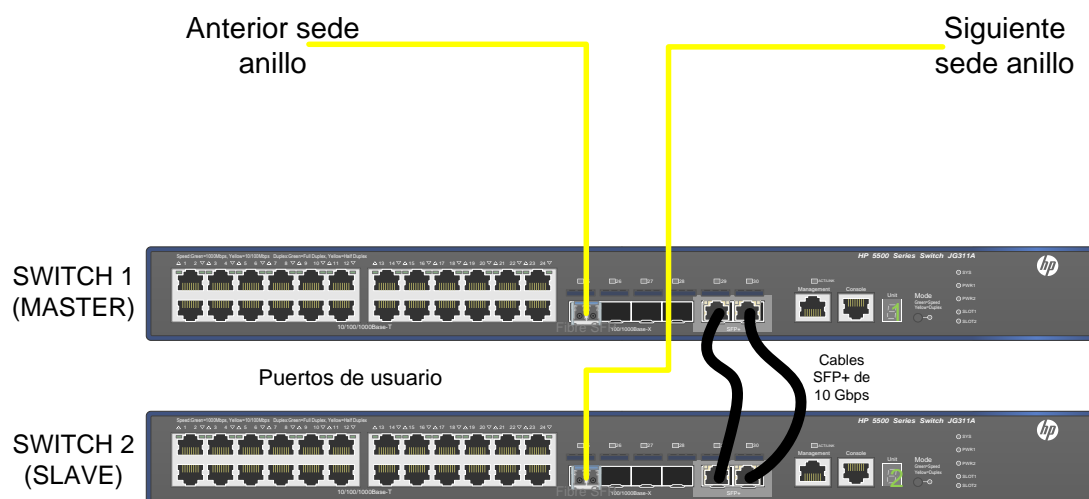


Figura 12: Clúster de Conmutadores en Anillo

Según como tenemos distribuido el anillo, tardaríamos actualmente en saber dónde se ha producido un corte de fibra o simplemente si un conmutador se ha apagado o se ha bloqueado, ya que todo seguiría funcionando con normalidad, eso sí utilizando una métrica más alta pero el usuario final no se daría cuenta. Por lo que, lo más probable es que nos cante el fallo cuando ya otro conmutador se quede sin conexión y dejemos aislado un sector del anillo. Ya que no hemos sido avisado de un primer corte.

A continuación, vamos a hablar de cómo nos conectamos a internet a través del anillo, bien pues en las 2 sedes principales que forman el anillo tenemos 2 DIBA de 100Mbps simétricas. DIBA es el servicio DataInternet, también llamado Data Internet Banda Ancha, es un servicio de acceso a internet para empresas de Telefónica. Al igual que MacroLAN y MetroLAN, se utiliza un enlace de fibra dedicado entre el domicilio del cliente y la central telefónica. Estas conexiones son realizadas por unos routers Juniper propios de telefónica y configurados por ellos. Todo el tráfico de internet es canalizado por un Fortigate 800C y sus entradas y salidas de red es lo que vamos a monitorizar de cada DIBA.

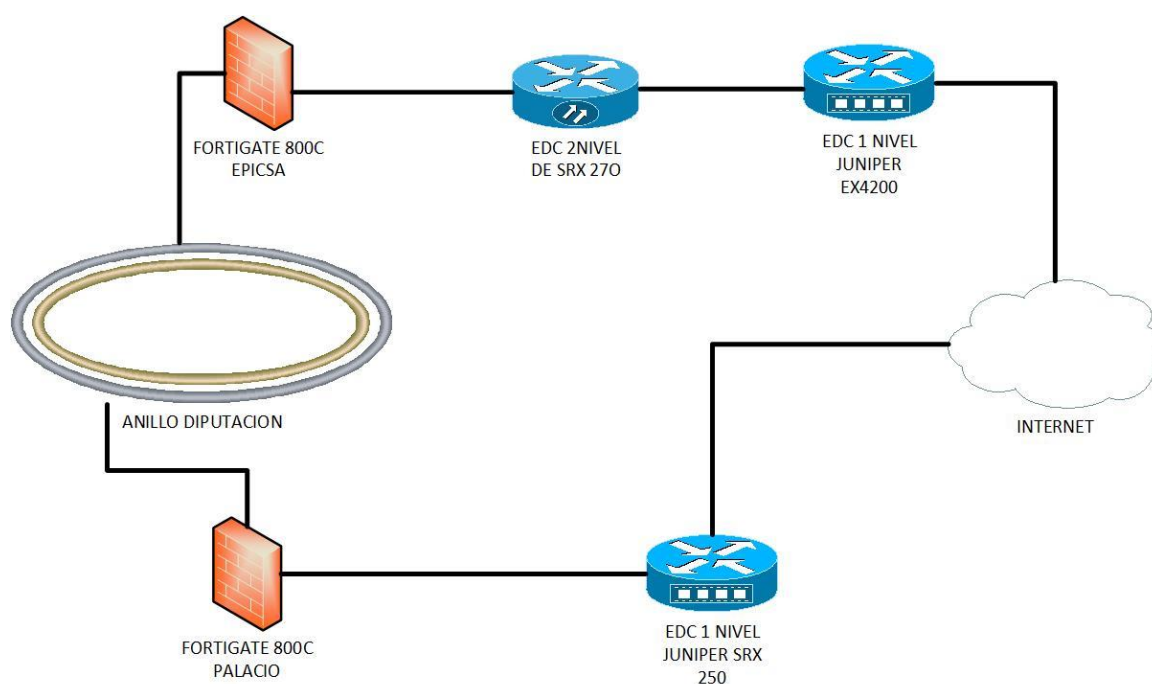


Figura 13: Acceso a internet Anillo

Est3 Fortigate 800c realiza la función de firewall para controlar el tráfico por ello van a ser nuestro referente si disponemos de internet en el anillo o no, ya que no podemos tener acceso inmediato a los juniper.



Figura 14: FORTIGATE 800c

1.3.2.2. VPN (Red Privada Virtual)

Otra situación que nos vamos a encontrar son los enlaces a las dependencias distribuidas por toda la provincia. Estas dependencias, son sedes de la propia Excma. Diputación de Cádiz, siendo una de ellas los ayuntamientos adheridos a los servicios de EPICSA. Dichos ayuntamientos, sólo pueden acceder a algunas aplicaciones a través de nuestra red, por ello se realizan enlaces a través de una Red Privada Virtual en estrella con EPICSA como nodo central de la red, con un caudal de 100Mbps simétrico agregado, sobre el que se cursa el tráfico de

datos corporativos de manera agregada con todas las sedes remotas. Esta red se basa en el servicio que pueda ofrecer el ISP en cada sede, por lo que actualmente van sobre DSL o Fibra, en la cual se garantiza en todo momento la robustez, seguridad y encriptación de los datos y para ello se emplean los servicios de Macrolan y VPN IP.

Para realizar la conexión en las sedes externas, es decir, en los ayuntamientos de la provincia de Cádiz adheridos a diputación, se utilizan Routers Cisco 877 K9, proporcionados y configurados por telefónica con un caudal mínimo de 2 Mbps simétrico. En EPICSA, al contratar el servicio DIBA anteriormente citado, recibimos un pool estático de direcciones públicas, y en nuestro caso obtenemos 4 direcciones y una de ella es utilizada para la conexión del servidor dedicado VPN



Figura 15: Router Cisco 877 k9

Cada una de estas sedes tendrá acceso a internet con otro enlace distinto al de EPICSA, lo vemos en la Figura 15. El servicio contratado para tener internet en cada ayuntamiento es contratado por el mismo. El router VPN es el que hace de puerta de enlace para los equipos de las sucursales. Y así, todo el tráfico que no va dirigido a EPICSA, es decir, que no sean peticiones corporativas las redirige al router de acceso a internet.

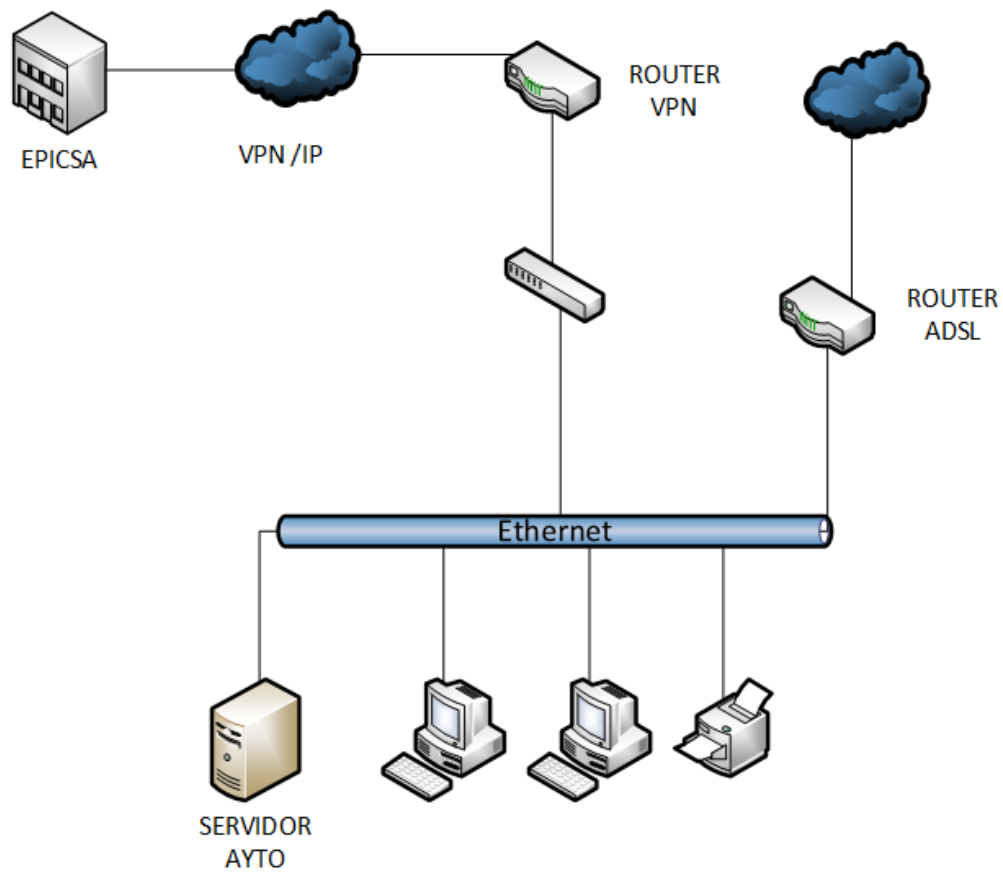


Figura 16: Sede externa al anillo

1.4. Normas y referencias

1.4.1. Disposiciones legales y normas aplicadas

Para la realización del proyecto nos basamos en las siguientes normativas:

- UNE 157801:2007 “Criterios generales para la elaboración de proyectos de sistemas de información ”
- Reglamento marco UCA/CG07/2012 de Trabajos Fin de Grado y Fin de Máster de la Universidad de Cádiz publicado en el BOUCA 148.

1.4.2. Programas utilizados

- Zabbix (Para la realización de la monitorización)
- Webmin (Para controlar el servidor)
- Putty (para realizar conexiones a través de ssh)
- Ubuntu Server (Como sistema operativo base del proyecto)
- MIB Browser (Programa para la búsqueda de códigos snmp)
- Google docs (para elaborar este documento)
- Microsoft Word (para elaborar este documento)
- Gantt Project (para elaborar el diagrama de Gantt)
- Dropbox (como copia de seguridad de documento)
- Microsoft Visio (para elaborar ilustraciones)

1.4.3. Bibliografía

Dalle Vacche, Andrea, y Stefano Kewan Lee. *Mastering Zabbix: Monitor Your Large IT Environment Efficiently with Zabbix*. First published. Packt Open Source. Birmingham: Packt Publ, 2013.

Gomez, Juan Fernando Duque. «Administracion De Redes y Mas: CONFIGURACION DE (SNMP) EN WINDOWS .» *Administracion De Redes y Mas*, 22 de marzo de 2012.
<http://infraestructurayserviciosdered.blogspot.com.es/2012/03/configuracion-de-snmp-en-windows.html>.

Olups, Rihards. *Zabbix 1.8 Network Monitoring: Monitor Your Network's Hardware, Servers, and Web Performance Effectively and Efficiently*. Birmingham: Packt Publ, 2010.

Uytterhoeven, Patrik. *Zabbix Cookbook: Over 70 Hands-on Recipes to Get Your Infrastructure up and Running with Zabbix*. Birmingham Mumbai: Packt Publishing, 2015.

«Zabbix Manual [Zabbix Documentation 3.0]». Accedido 8 de junio de 2017.
<https://www.zabbix.com/documentation/3.0/manual>.

«Anexo:Comparación de sistemas de monitorización de redes». *Wikipedia, la enciclopedia libre*, 18 de abril de 2017.
https://es.wikipedia.org/w/index.php?title=Anexo:Comparaci%C3%B3n_de_sistemas_de_monitorizaci%C3%B3n_de_redes&oldid=98447327.

«Campus_Cisco_Resumen_Diseño.pdf». Accedido 27 de junio de 2017.
http://www.cisco.com/c/dam/r/es/la/internet-of-everything-ioe/assets/pdfs/en-05_campus-wireless_wp_cte_es-xl_42333.pdf.

«El modelo jerárquico de 3 capas de Cisco». *IP reference*, 28 de noviembre de 2008. <https://ipref.wordpress.com/2008/11/28/modelo-jerarquico-de-red/>.

«EPICSA». Accedido 3 de julio de 2017.
<http://www.dipucadiz.es/epicsa/EPICSA/>.

«Nagios y Zabbix — Soluciones De Monitoreo De Código Libre». *Información práctica sobre Redes, Linux, Seguridad y Hacking para profesionales de TI. Capacity Academy*, 26 de diciembre de 2013.

<http://blog.capacityacademy.com/2013/12/26/nagios-zabbix-soluciones-de-monitoreo-ti-de-codigo-libre/>.

«OID description for 1.3.6.1.2.1.1.5.0 - sysName». Accedido 30 de junio de 2017.

<http://www.alvestrand.no/objectid/1.3.6.1.2.1.1.5.0.html>.

«Packt.Mastering.Zabbix.Dec.2013.ISBN.1783283491.pdf», s. f.

«Submodelo de información en OSI». Accedido 30 de junio de 2017.

<http://www.arcesio.net/osinm/osinminformacion.html>.

1.5. Definiciones y abreviaturas

EPICSA:

Empresa Provincial de Información de Cádiz Sociedad Anónima.

TIC:

Tecnología de la información y Comunicaciones.

CPD:

Centro de procesamiento de datos.

Anillo Metropolitano:

Una red en anillo es una topología de red, en la que cada nodo tiene una única conexión hacia los nodos adyacentes, formando así, un anillo repartido por toda la ciudad y en este caso de fibra óptica dedicada.

VPN:

Una red privada virtual es una tecnología que crea una conexión cifrada a través de una red menos segura como es internet.

SMS

“Short Message Service” Servicio de mensajes cortos o simples.

SNMP

“Simple Network Management Protocol” Protocolo simple de administración de red

WAN

“Wide Area Network” Red de área ampliada, es una red privada de telecomunicaciones

DIBA

“DataInternet”, también llamado Data Internet

Banda Ancha, es un servicio de acceso a internet para empresas de Telefónica.

VLAN

“Red de área local virtual” es una red lógica dentro una red física

1.6. Requisitos Iniciales

El departamento de sistemas y redes, nos indica qué es lo que quieren monitorizar en un primer momento, y de qué manera quieren que nos avisen de las alertas de monitoreo. Fundamentalmente, los avisos de alerta llegarán mediante correo electrónico pero también, cabe la posibilidad de intentar que las alertas nos la indiquen por SMS o por mensajería instantánea.

Por otro lado, también nos indica la importancia de utilizar software libre de monitorización.

Servidores:

Como anteriormente se ha dicho, en estos equipos podemos distinguir dos grandes grupos, servidores de producción y servidores de desarrollo. Además los equipos que nos interesan monitorizar están bajo Linux y Windows, por lo que también obtendremos otros 2 sub-grupos.

De estos equipos se quiere saber la disponibilidad de ellos en todo momento, la memoria RAM que tiene el equipo y cuanto está utilizando en un momento dado. De igual manera, también es importante saber la capacidad de disco duro que tiene y cuanto queda por consumir. Por otra parte, también es interesante la carga de del procesador que tiene actualmente, así como el número de procesos que está corriendo. Además de ello, se requiere que nos dé un aviso de alerta, en principio a través de correo electrónico.

Todos estos equipos, no se encuentran únicamente en el CPD sino que también podemos encontrar en los distintos ayuntamientos que tenemos por la provincia gaditana. Estos equipos suelen ser servidores de dominio y están bajo Windows.

Redes

Se quiere monitorizar el anillo completo de la diputación de Cádiz, es decir, los puntos de enlaces que tenemos de una sede a otra completando el anillo. En principio, se quiere saber en cada momento el estado del enlace, cómo está, si está correcto o tenemos un percance, que como nos comunica puede ser un corte de fibra, perdida del suministro eléctrico etc... Al igual que estamos monitorizando el estado activo del anillo, también tendremos que monitorizar los accesos a internet que tiene la diputación, siendo estos en la sede de diputación Palacio y

el enlace que se encuentra en EPICSA. Además hay sedes que también cuelga del anillo que serían interesante tener monitorizadas.

Otra situación que tenemos que controlar es las conexiones con los distintos centros repartidos por la provincia de Cádiz, tanto ayuntamientos como centros de la propia diputación. De estos centros tenemos que controlar el acceso VPN que tienen con EPICSA y la salida a internet.

1.7. Alcance del proyecto

El alcance de este proyecto abarca la monitorización de red del anillo metropolitano dedicado que dispone EPICSA, es decir, saber en cada momento si el enlace entre sedes está disponible y para ello se monitoriza los conmutadores de red que realiza los enlaces para completar el anillo.

Otro objetivo, es la red en estrella que tiene dedicada con los ayuntamientos de la provincia de Cádiz a través de conexiones VPN, así como cada uno de los servidores de cada ayuntamiento y su conexión a internet.

Y la monitorización de los servidores físicos y virtuales que actualmente se encuentra en el Centro de Proceso de Datos (en adelante CPD).

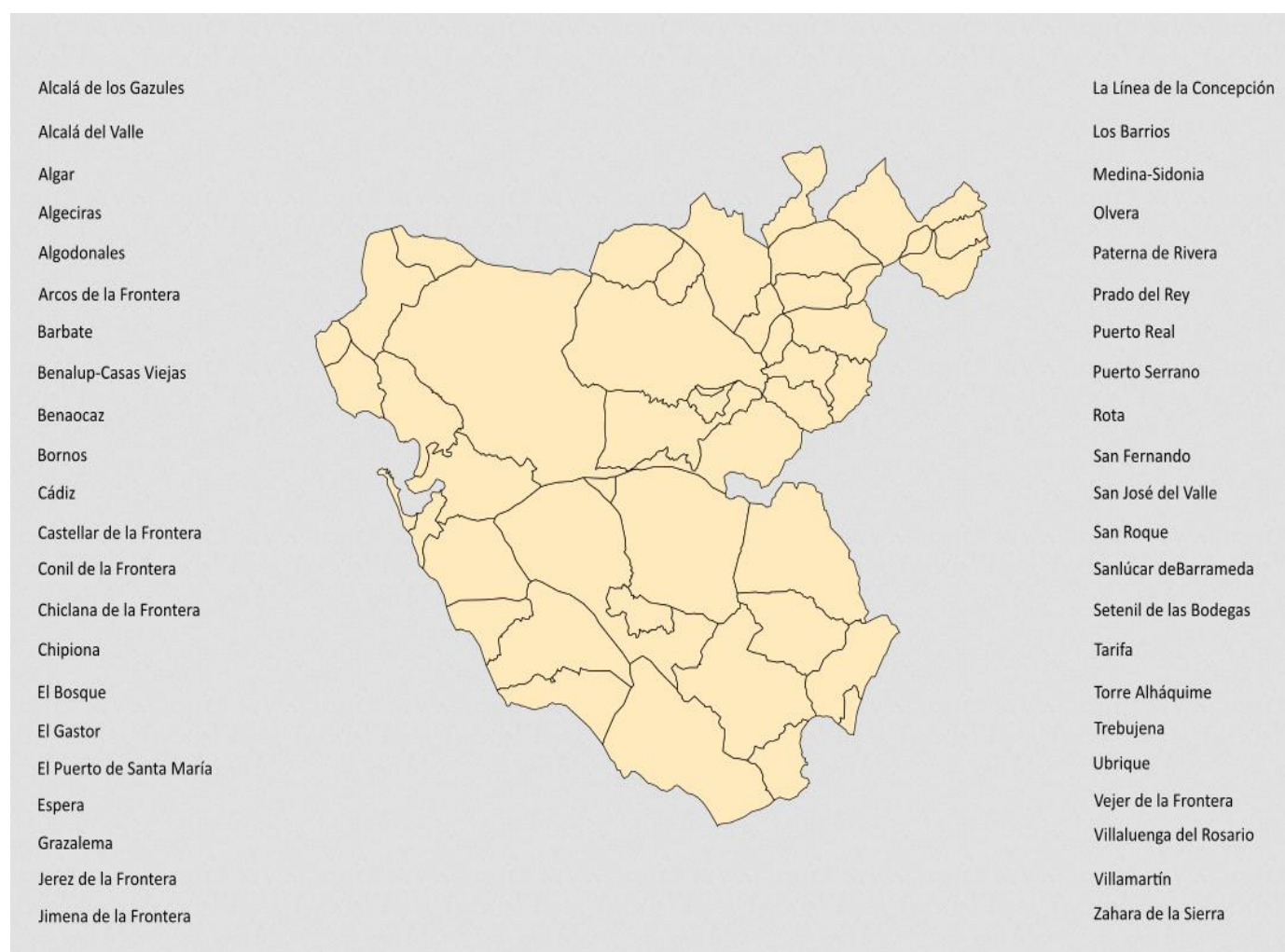


Figura 17: Mapa provincia de Cádiz con centros

No está en el alcance del proyecto monitorizar el enlace de red con los usuarios finales, ni sus propios equipos, ni la infraestructura de red de los ayuntamientos.

1.8. Estudios de alternativas y viabilidad

Nos disponemos a tratar distintas soluciones para afrontar los requisitos que se nos ha planteado para la realización de este proyecto, teniendo en cuenta que tenemos que realizarlos con un software libre.

1.8.1. Estudio de Software a utilizar

1.8.1.1. Alternativa 1 administrador

Cacti:

Herramienta de software libre y posible solución de administración para dispositivos en red. Dispone de interfaz web 2.0 basado en AJAX, plugins integrados en el núcleo de la aplicación, grupos de usuarios y permisos, etc. Está publicada bajo la licencia GPL (GNU Public Licensed).

No dispone de una versión comercial ni otra licencia privativa para la distribución del producto, tampoco de un soporte comercial o profesional. Pone a disposición un soporte gratuito mantenida por la comunidad. Sirve para monitorizar redes en LAN de un tamaño pequeño o redes más amplias de hasta cientos de dispositivos. La recopilación de datos en los dispositivos a monitorizar se realiza mediante el protocolo SNMP y se almacena en una base de datos RRD. Permite el acceso mediante usuarios con diferentes privilegios, para darle permisos sobre ciertas áreas de Cacti.

Ventajas:

- Es una herramienta avanzada para la generación de gráficas y utiliza una tecnología libre también fomentada por otras herramientas como es RRDtool.

Inconvenientes:

- tiene un potencial inferior a otras herramientas de monitorización de servicios
- No cumple con funcionalidades básicas como la monitorización de hardware (CPU, memoria, disco, etc.)
- Su interfaz web no permite controlar la aplicación sólo permite una visualización de los datos obtenidos.

1.8.1.2. Alternativa 2 administrador

Nagios:

El principal software libre orientado a la monitorización. Es una herramienta Open Source y está diseñado y mantenido por Ethan Galstad, autor de dicho software. Está licenciado bajo la GNU General Public License.

En cuanto a su arquitectura y definición, es un sistema de monitorización monolítico y orientado a eventos que vigila los equipos, tanto su hardware como software, alertando cuando el comportamiento de los mismos no es el adecuado. Puede monitorizar servicios de red, recursos hosts y puede programar plugins específicos para nuevos sistemas. El control remoto es manejado a través de túneles SSH o SSL cifrado. Fue diseñado para sistemas GNU/Linux pero también funciona en variantes Unix.

Está basado en una estructura maestro-esclavo donde el maestro es el servidor dedicado para Nagios y los esclavos las máquinas a monitorizar.

Ventajas:

- Es un software popularmente conocido y consolidado, ya que posee una gran cantidad de plugins de la comunidad.
- Permite diferenciar entre hosts caídos o inaccesibles.
- Posee un comando que chequea y valida los ficheros de texto de configuración modificados antes de reiniciar el sistema.
- Puede acoplarse con otra aplicación llamada Centreon para la gestión y control de cualquier aspecto de la herramienta desde una interfaz web, evitando las modificaciones sobre ficheros y por línea de comandos.

Inconvenientes:

- La instalación, configuración y los complementos (plugins) está basada en texto, lo cual implica una dificultad media, inversión de tiempo y requiere un grado de conocimiento técnico, además puede resultar algo tedioso.
- Cualquier modificación en la configuración requiere un reinicio completo del sistema.
- Su interfaz web sólo sirve para visualizar los acontecimientos. Cualquier cambio debe realizarse manualmente desde el servidor de Nagios.

- No soporta ningún gestor de base de datos que trabaje bajo SQL.
- No está disponible o no funciona en todos los sistemas operativos, por ejemplo, en sistemas Microsoft Windows
- Su arquitectura se basa en un único proceso para realizar diferentes tareas.

1.8.1.3. Alternativa 3 administrador

Zabbix

Nos permite tener toda la información (hasta 10000 nodos) de monitorización en tiempo real y la configuración centralizada en un solo servidor, podemos acceder a los informes mediante un navegador web.

Entre otras muchas cosas Zabbix puede descubrir los nodos en un rango de IPs mediante agentes SNMP. Puede monitorizar servicios remotos, tiene soporte para traps SNMP y SNMP v1, 2,3. Además de proporcionar extensa información sobre la máquina: disco, memoria, E/S ...

Permite la monitorización de recursos hardware: procesos de carga, actividad en la red, actividad en disco, parámetros del sistema operativo, servicios de red (SMTP, HTTP), soporte para la monitorización remota o sin agentes a través de: SNMP, ICMP, TCP, IPMI, SSH y Telnet. Genera informes y estadísticas y la posible visualización de los datos a través de su interfaz web, la cual está desarrollada en PHP y JavaScript.

Sus principales elementos o componentes son:

Una base de datos, que soporta MySQL, PostgreSQL, SQLite, Oracle o IBM DB2 para almacenar los datos.

Su servidor Zabbix y sus agentes Zabbix, los cuales están desarrollados en lenguaje C. Incluye algunas características destacadas:

- Auto detección de dispositivos y servicios monitorizados.
- Monitorización en tiempo real: rendimiento, disponibilidad, integridad, registro de logs, etc.
- Servicios IT jerárquicos.

Ventajas:

- Ofrecen una web en distintos idiomas muy bien organizada:
www.zabbix.com
- Tienen en mente el crecimiento de la comunidad Zabbix, poniendo a disponibilidad una wiki en construcción.

- Facilidad de usar es intuitivo.
- Contiene distintas formas de monitorización SNMP, propio agente, JMX, IPMI

Inconvenientes:

- La potencia o capacidad del software es menor que la de alguno de los mencionados anteriormente
- El no disponer de una versión Enterprise hace que no crezca tanto su popularidad en cuanto a clientes importantes asociados a la herramienta.

1.8.1.4. Alternativa Solución administrador

Vamos a realizar una rápida tabla comparativa de los tres sistemas seleccionados para la monitorización de EPICSA, e indicaremos cual elegimos para realizar el proyecto.

SISTEMAS DE MONITORIZACIÓN	Software libre	Funcionalidad	Fácil uso	Arquitectura	Soporte	Agente
NAGIOS	SI	SI	NO	NO	SI	SI
CACTI	SI	SI	NO	NO	NO	NO
ZABBIX	SI	SI	SI	NO	SI	SI

Tabla 2: Comparativa Software Monitorización

Tras el estudio de las varias alternativas para realizar el proyecto de monitorización se ha decidido utilizar la herramienta ZABBIX. Además de las opciones que vemos reflejada en la tabla, se ha decidido dicha herramienta porque tiene un mayor campo de monitorización que el resto, no sólo se va a poder monitorizar por agente como en otras herramientas, sino que además de disponer de un propio agente para los casos que veamos oportuno, también vamos a poder

monitorizar por SNMP, IPMI, JMX, monitorizar escenarios web, etc.; consiguiendo así un mayor campo de monitorización.

Su interfaz gráfica también es una gran ventaja. Desde ella se puede realizar todas las configuraciones posibles que tiene ZABBIX. Tiene una amplia gama de gráficos para poder utilizar en nuestros mapas personalizados, y además, podemos añadir tanto nuevos iconos como fondos.

Otra de las opciones que nos hace decantarnos por ZABBIX es la capacidad de tomar acciones que le indiquemos. No sólo es capaz de enviarnos un SMS o un correo electrónico entre otras, sino que cuando algo falla, también es capaz de ejecutar un script para poder levantar un servicio caído. Por ejemplo, si tenemos una página web, que el tomcat no responde correctamente y nos da fallo en su monitor establecido podrá enviarle el script para ejecutarlo instantáneamente para levantar el servicio y así, no tener que interactuar el administrador del sistema.

Como otra característica más para decantarnos por ZABBIX, es su amplia comunidad.

1.8.2. Estudio Monitorización de equipos

Ahora vamos a ver cómo monitorizar los servidores. Para ello tenemos la opción de monitorizarlos con SNMP o con Agente ZABBIX, pero a su vez tendremos que elegir qué tipo de agente utilizar, activo o pasivo.

Con respecto a monitorizar los equipos con SNMP o ZABBIX, siempre que podamos instalar el agente en el equipo es la mejor opción, ya que no tendría que estar buscando los códigos MIBS para su utilización.

Otra característica que nos hace decantarnos por el propio agente es su seguridad ya que es menos conocido que el SNMP y mucho más seguro. Y el agente ZABBIX tiene un gran abanico de posibilidades a monitorizar, y con respecto a lo que vamos a monitorizar, es más que suficiente.

Ahora vamos a contemplar la opción de agente activo o agente pasivo para los servidores, tanto sea Windows o Linux ya que disponemos de agente para ambos.

Agente activo:

El agente indica las opciones de monitorización que tiene disponible cada cierto tiempo y el servidor le hace la petición de todo lo que quiere monitorizar en conjunto y a continuación el agente se lo envía.

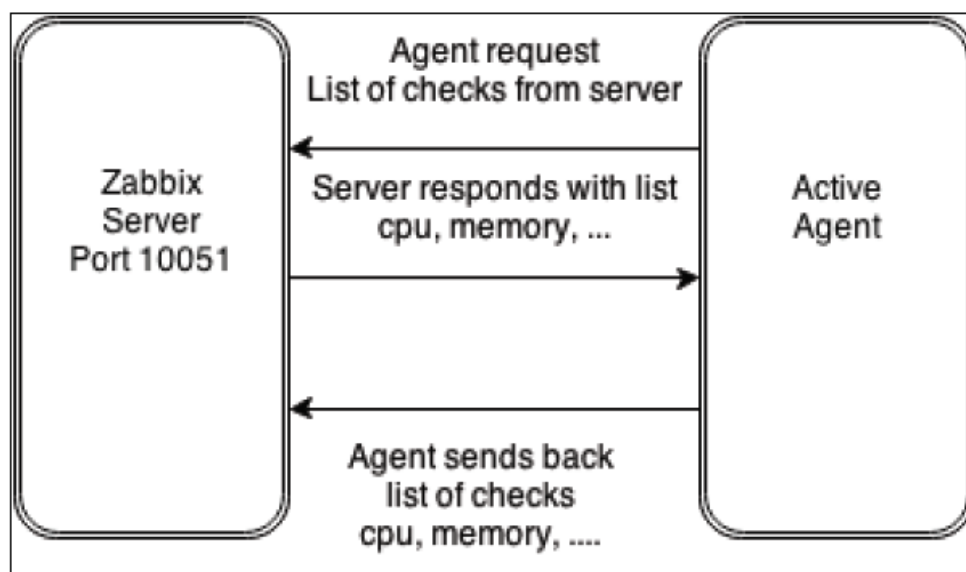


Figura 18: ZABBIX agente activo

Agente pasivo:

El servidor ZABBIX le indica al agente lo que quiere monitorizar pero las peticiones son de una en una por lo que puede tener más tiempo la red ocupada

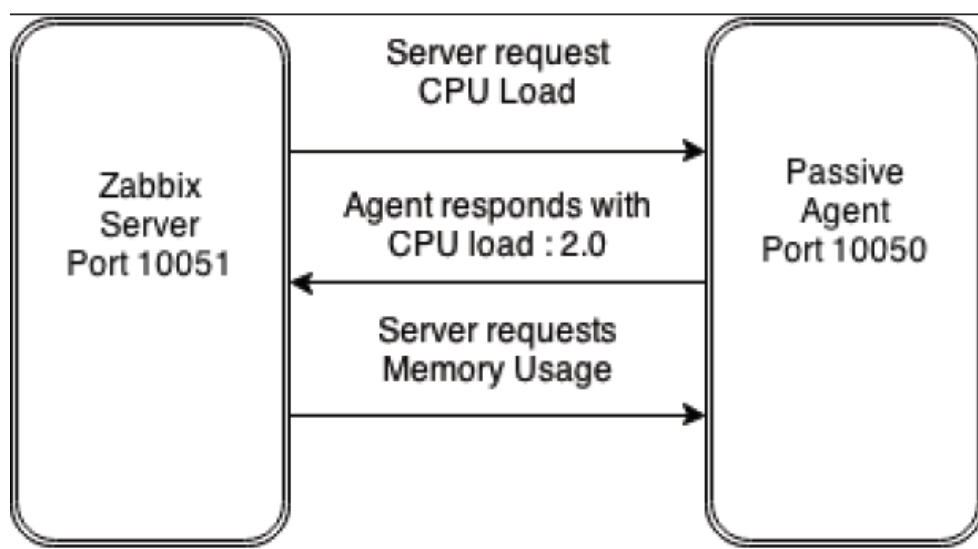


Figura 19: ZABBIX agente pasivo

Tras la comparativa que hemos visto, nos hemos decantado por la opción de utilizar el agente ZABBIX pasivo. Ya que muchas comprobaciones que vamos a realizar no tienen que ser continuas, es decir, algunas comprobaciones las haremos una vez en semana, mientras que otras las podemos hacer cada minuto, por lo que no nos interesa que nos esté mandando información continua de todo cuando no es necesario.

Para los equipos que no tienen soporte de agente ZABBIX vamos a utilizar snmp para su monitorización y especialmente su versión 2. Esto nos llevaría a debatir que por qué no la versión 3, ya que es más segura, pero no todo los aparatos los soporta, y tenemos mucha más documentación de SNMP v2.

También podremos encontrarnos con otra situación, y es que nos podemos encontrar con dispositivos que por restricciones de seguridad no le podremos activar agente ZABBIX y tampoco el SNMP. Entonces, vamos a realizar la monitorización a través de una comprobación sencilla como por ejemplo que la interfaz de red nos contesta a un simple ping.

1.9. Descripción de la Solución propuesta

Tras la decisión realizada para abordar el proyecto procederemos a indicar los pasos a realizar para el correcto funcionamiento del programa de monitorización, tanto en los medios a monitorizar como el propio servidor, ya que tendremos que preparar un sistema operativo con los requisitos que conlleva ZABBIX.

En primer lugar vamos a indicar qué es lo que vamos a monitorizar, y con qué herramienta se va realizar el seguimiento si SNMP, agente ZABBIX.

Equipos / Servicios	Monitorización
HP-A5500	SNMP
FORTIGATE	SNMP
NODOS_AYTOS	AGENTE ZABBIX, Comprobación Simple
SAI (Medir temperatura CPD)	SNMP
LINUX_PRODUCCIÓN	AGENTE ZABBIX
LINUX_DESARROLLO	AGENTE ZABBIX
WINDOWS_PRODUCCIÓN	AGENTE ZABBIX
WINDOWS_DESARROLLO	AGENTE ZABBIX
PORTALES WEB	SCENARIOS WEB

Tabla 3: Equipos a Monitorizar

1.9.1. Elementos a monitorizar

Vamos a indicar qué es lo que se va a monitorizar de cada grupo de equipo por forma general y además, indicaremos cuándo se crearan alertas y de qué manera se le avisará al administrador. Ya que cada iniciador tiene que estar relacionado con un monitor, lo que se realiza es, advertir sobre un monitor que no nos está dando un valor esperado y a partir de ese momento ahora podemos decir cómo quiere que nos notifique si por correo o SMS.

Tenemos en cuenta que algún servidor puede tener más necesidades que las que se especifican aquí generalmente, pero en primer lugar, todos debe tener monitorizado lo que a continuación especificamos.

Equipos	Monitores	Iniciadores	Tipo de Aviso
HP-A5500	Interfaz de red a nodos adyacentes Localización Nombre	Si alguna interfaz de red que conecta los nodos del anillo se cae. Si el equipo no responde	Correo SMS
FORTIGATE	Verificar estado de cada DIBA. Ver el tráfico que genera cada una	Que no tengamos tráfico en alguna interfaz.	Correo SMS
SAI CPD	Medimos la Temperatura	Advertencia de temperatura mayor de 29°C Advertencia de temperatura mayor 25 °C	Correo SMS
LINUX PRODUCCIÓN	Memoria Unidades de almacenamiento Carga del procesador Estado del equipo	Poco espacio en memoria y unidades Avisar si el equipo no está disponible	Correo
LINUX DESARROLLO	Tiempo equipo en corriendo	Carga de CPU alta	
WINDOWS PRODUCCIÓN	Memoria Unidades de almacenamiento Carga del procesador	Poco espacio en memoria y unidades Avisar si el equipo no está disponible	Correo
WINDOWS DESARROLLO	Estado del equipo Tiempo equipo en corriendo	Carga de CPU alta	

PORTALES WEB	Se monitorizan a través de escenarios web y lo que vamos a comprobar es el acceso a esa web. En el caso de la intranet vamos a comprobar el login	Si nos da un condigo de error al acceder a la web	Correo
NODOS AYUNTAMIENTOS	Memoria Unidades de almacenamiento Carga del procesador Estado del equipo Tiempo equipo en corriendo Estado de conexión con la VPN y INTENET	Poco espacio en memoria y unidades Avisar si el equipo no está disponible Carga de CPU alta Si las conexiones de VPN o INTERNET no se encuentran disponibles	Correo

Tabla 4: Elementos a Monitorizar

1.9.2. Plantillas de equipos y especificación

Como contamos con una gran cantidad de servidores similares, realizaremos unas plantillas que podemos asignar a los equipos y así facilitar un poco el trabajo. En vez de realizar la configuración por equipo, la realizaremos por grupos. Se realizaran las siguientes plantillas:

- PLANTILLA WINDOWS GENERICA
 - Esta plantilla la contendrá los grupos de:
 - Windows Producción
 - Windows Desarrollo
 - Nodos Ayuntamientos
 - Realizamos los siguientes monitores :

Sistema Activo	Iniciadores 1	system.uptime
Memoria Total		vm.memory.size[total]
Información del equipo	Iniciadores 1	system.uname
Carga procesador	Iniciadores 1	system.cpu.util[,user,avg1]
Numero de procesos	Iniciadores 1	proc.num[]
Numero de hilos		perf_counter[2\250]
Memoria disponible	Iniciadores 1	vm.memory.size[free]

Figura 20: Monitores Windows

- Realización de los siguientes iniciadores:

<input type="checkbox"/> GRAVEDAD	NOMBRE ▼	EXPRESIÓN
<input type="checkbox"/> Medio	{HOSTNAME}: Carga de CPU alta	{PLANTILLA WINDOWS GENERICA:system.cpu.util[,user,avg1].avg(300)}>50
<input type="checkbox"/> Medio	{HOST.NAME} poca memoria disponible	{PLANTILLA WINDOWS GENERICA:vm.memory.size[free].last(0)}<10000
<input type="checkbox"/> Alta	{HOST.NAME} No esta disponible	{PLANTILLA WINDOWS GENERICA:system.uname.nodata(90)}<>0
<input type="checkbox"/> Medio	{HOST.NAME} El equipo se ha reiniciado	{PLANTILLA WINDOWS GENERICA:system.uptime.change(0)}<0
<input type="checkbox"/> Medio	{HOST.NAME} Demasiados procesos corriendo	{PLANTILLA WINDOWS GENERICA:proc.num[].avg(5m)}>300

Figura 21: Iniciadores Windows

- Realizaremos las siguientes Gráficas de los monitores:
 - Memoria disponible
 - Carga del procesador

- PLANTILLA LINUX GENERICA
 - Esta plantilla la contendrá los grupos de:
 - Linux Producción
 - Linux Desarrollo
 - Realizamos los siguientes monitores :

NOMBRE	INICIADORES	MONITOR
Memoria total		vm.memory.size[total]
Numero de procesos corriendo		proc.num[]
Uptime del Equipo	Iniciadores 1	system.uptime
Version del zabbix_agent(d) corriendo		agent.version
Memoria Libre	Iniciadores 1	vm.memory.size[free]
Informacion del Sistema	Iniciadores 1	system.uname
Espacio libre en / en %	Iniciadores 2	vfs.fs.size[/,pfree]
Espacio swap libre		system.swap.size[, free]
Espacio total en /		vfs.fs.size[/,total]
Espacio total swap		system.swap.size[,total]
Carga Procesador	Iniciadores 1	system.cpu.util[,user,avg1]

Figura 22: Monitores Linux

- Realización de los siguientes iniciadores:

<input type="checkbox"/> GRAVEDAD	NOMBRE ▼	EXPRESIÓN
<input type="checkbox"/> Alta	{HOSTNAME}: Falta de memoria libre	{PLANTILLA LINUX GENERICA:vm.memory.size[free].last(0)}=10000
<input type="checkbox"/> Medio	{HOSTNAME}: El equipo ha sido reiniciado	{PLANTILLA LINUX GENERICA:system.uptime.last(0)}<600
<input type="checkbox"/> Alta	{HOSTNAME}: Carga de CPU alta	{PLANTILLA LINUX GENERICA:system.cpu.util[,user,avg1].avg(300)}>50
<input type="checkbox"/> Medio	{HOSTNAME}: 10% de espacio libre en /	{PLANTILLA LINUX GENERICA:vfs.fs.size[/,pfree].last(0)}<10
<input type="checkbox"/> Alta	{HOSTNAME}: 5% de espacio libre en /	{PLANTILLA LINUX GENERICA:vfs.fs.size[/,pfree].last(0)}<5
<input type="checkbox"/> Alta	{HOST.NAME} No esta disponible	{PLANTILLA LINUX GENERICA:system.uname.nodata(90)}<>0

Figura 23: Iniciadores Linux

- Realizaremos las siguientes Gráficas de los monitores:
 - Grafica de CPU

- Espacio libre disco
- Memoria Libre
- PLANTILLA RED HP
 - Esta plantilla contendrá el siguiente grupo
 - HP-A5500
 - Realizamos los siguientes monitores:

<input type="checkbox"/>	WIZARD	NOMBRE	INICIADORES	MONITOR	INTERVAL
<input type="checkbox"/>	...	Localizacion		LocalizacionSW	10m
<input type="checkbox"/>	...	Nombre	Iniciadores 1	NombreSW	10m

Figura 24: Monitores HP

- Y el siguiente Iniciador:

<input type="checkbox"/>	GRAVEDAD	NOMBRE ▼	EXPRESIÓN
<input type="checkbox"/>	Alta	{HOST.NAME} No esta disponible	{PLANTILLA_RED_HP:NombreSW.nodata(900)}<>0

Figura 25: Iniciadores HP

- PLANTILLA LINUX APACHE
 - Esta plantilla la contendrá algunos equipos de los grupos:
 - Linux Producción
 - Linux desarrollo
 - Realizamos el siguiente monitor:

<input type="checkbox"/>	WIZARD	NOMBRE	INICIADORES	MONITOR ▲
<input type="checkbox"/>		APACHE Puerto 80 caído	Iniciadores 1	proc.num[httpd,,,/opt /apache/bin]

Figura 26: Monitor Apache

- Y el siguiente Iniciador:

<input type="checkbox"/> GRAVEDAD	NOMBRE ▾	EXPRESIÓN
<input type="checkbox"/> Crítica	Proceso APACHE PUERTO 80	{PLANTILLA_LINUX APACHE:proc.num[httpd,,,/opt/apache/bin].last()}<1

Figura 27: Iniciador Apache

- PLANTILLA LINUX APACHE2410
 - Esta plantilla la contendrá algunos equipos de los grupos:
 - Linux Producción
 - Linux desarrollo
 - Realizamos el siguiente monitor:

<input type="checkbox"/> WIZARD	NOMBRE	INICIADORES	MONITOR ▲	INTERVAL
<input type="checkbox"/>	APACHE Puerto 80 caído	Iniciadores 1	proc.num[httpd,,,/opt /apache2410/bin]	30s

Figura 28: Monitor Apache 2410

- Y el siguiente Iniciador:

<input type="checkbox"/> GRAVEDAD	NOMBRE ▾	EXPRESIÓN
<input type="checkbox"/> Crítica	Proceso APACHE PUERTO 80	{PLANTILLA_LINUX APACHE2410:proc.num[httpd,,,/opt/apache2410/bin].last()}<1

Figura 29: Iniciador Apache 2410

- PLANTILLA LINUX DSMCAD
 - Esta plantilla la contendrá algunos equipos de los grupos:
 - Linux Producción
 - Linux desarrollo
 - Realizamos el siguiente monitor:

<input type="checkbox"/>	WIZARD	NOMBRE	INICIADORES	MONITOR ▲	INTERVAL
<input type="checkbox"/>		Proceso DSMCAD	Iniciadores 1	proc.num[dsmcad,,,/opt/tivoli/tsm/client/ba/bin/dsmcad]	10m

Figura 23: Monitor DSMCAD

- Y el siguiente Iniciador:

<input type="checkbox"/>	GRAVEDAD	NOMBRE ▼	EXPRESIÓN
<input type="checkbox"/>	Alta	{HOSTNAME}: Proceso Tivoli (dsmcad) caído	{PLANTILLA_LINUX DSMCAD:proc.num[dsmcad,,,/opt/tivoli/tsm/client/ba/bin/dsmcad].last()}<1

Figura 31: Iniciador DSMCAD

- PLANTILLA LINUX POOL OFFICE
 - Esta plantilla la contendrá algunos equipos de los grupos:
 - Linux Producción
 - Linux desarrollo
 - Realizamos el siguiente monitor:

<input type="checkbox"/>	WIZARD	NOMBRE	INICIADORES	MONITOR ▲	INTERVAL
<input type="checkbox"/>		Pool OPEN-OFFICE	Iniciadores 1	proc.num[java,,,ooo_server1_1_1.jar]	1m

Figura 32: Monitor POOL OFFICE

- Y el siguiente Iniciador:

<input type="checkbox"/>	GRAVEDAD	NOMBRE ▼	EXPRESIÓN
<input type="checkbox"/>	Alta	{HOSTNAME}: Proceso Pool Soflice caído	{PLANTILLA_LINUX POOL OFFICE:proc.num[java,,,ooo_server1_1_1.jar].last()}<1

Figura 33: Iniciador POOL OFFICE

1.9.3. Escala de valores de incidencias

Ahora vamos a indicar la escala de valores que tomaremos para clasificar un iniciador, que lo que conlleva es un evento no esperado en el sistema de un monitor. Para ello tenemos los siguientes valores menor gravedad a mayor:

- Sin Clasificar
 - No es nada importante pero está ahí
- Informativa
 - Nos da solo información de lo que está sucediendo y puede ir a mas
- Advertencia
 - La tomaremos como algo muy leve
- Media
 - Hay que investigar qué es lo que sucede para poner una solución a medio plazo.
- Alta
 - Tenemos que solucionar el problema lo antes posibles
- Critica
 - Es de actuación inmediata

Esta representación de valores nos sirve para la toma de decisiones como filtro para realizar una acción sobre el problema, como por ejemplo enviar un correo o la ejecución de un script.

1.9.4. Acciones del sistema

Una vez ya configurados los equipos con el agente o activación de SNMP, como veremos en el anexo 8, la realización de los monitores con sus respectivos iniciadores, se pasa a construir las acciones cuando se detecta algo no habitual.

Tenemos actualmente varias opciones que son las siguientes:

- Envíos de SMS que se va a utilizar exclusivamente para los eventos críticos
- Envío de correo electrónico que se van a realizar para las gravedades media, alta, critica.
- Ejecución de script en maquina con problemas, esta opción la vamos a utilizar para las caída de los servicios. Y realmente lo que hace es enviar una instrucción que se ejecuta en el equipo de destino. Ponemos un ejemplo nos llega la alerta que el servicio tomcat se ha caído, pues se envía el comando para reiniciar automáticamente el servicio.

Una acción puede conllevar más de una operación y además podemos indicar que cuando se recupere del problema también nos avise. Además tenemos la posibilidad de enviar el mensaje a las personas o departamentos afectados. Para el envío de las acciones es necesario registrar a los usuarios que van a recibir los eventos. Así como dar de alta los medios de envío.

1.9.5. Administración usuarios y tipos de medio

Vamos a empezar con los tipos de medios que se crearan. Éstos son SMS y Correo electrónico. No vamos a entrar a explicar cómo se configura en esta sección, ya que lo podemos ver en el anexo 9, configuración de tipos de medios.

Lo que si vamos a indicar es como como vamos a estructurar los usuarios.

Vamos a crear un grupo en el que engloba el departamento de sistemas y redes, pero a su vez vamos a crear un usuario por cada sub departamento. Para que solo sea notificado cada administrador cuando sea necesarios, se realizará un grupo para los administradores de ZABBIX que de momento solo contará con un único usuario, que es el encargado del mantenimiento de la plataforma.

Además de utilizar los usuarios para enviar notificaciones, le podemos dar acceso a la aplicación, pero incluso se le puede otorgar solo los permisos que sean necesarios para su visualización o control.

1.9.6. Diseño de mapas interactivos

Para que nuestro proyecto sea un poco más amigable vamos a indicar qué mapas vamos a realizar y qué conseguiremos con ello, ya que podremos interactuar con los mapas para llegar a ver qué es lo que ocurre en una zona determinada.

En primer lugar, hemos decidido realizar un mapa de inicio con 4 componentes esenciales, que serían CPD, anillo metropolitano, sedes remotas y como no, nuestro servidor ZABBIX. Cada uno de estos nodos están asociados a un segundo mapa, para representar mejor las diferentes zonas que se interactúan.

En caso de que se detecte una incidencia o más, el fondo del icono tendrá el color de la incidencia más alta que esté en el mapa asociado al nodo, veamos un ejemplo con la siguiente ilustración.

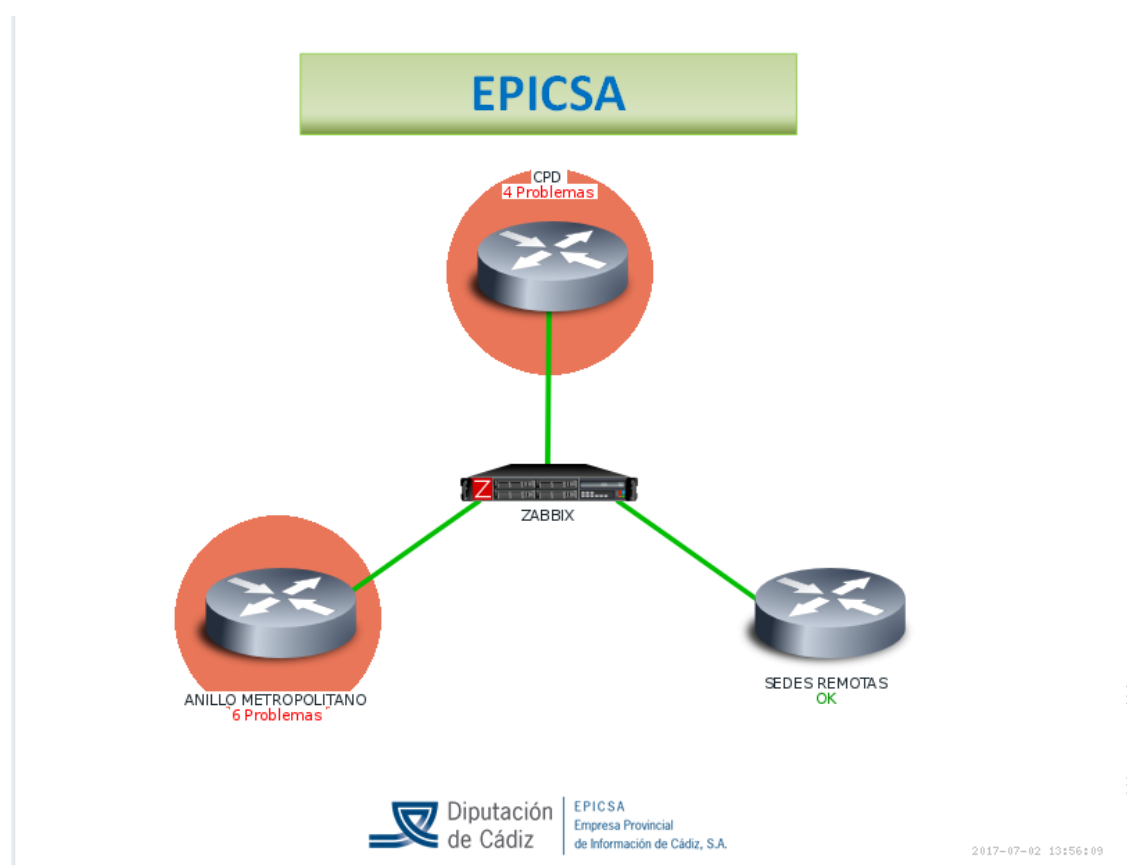


Figura 34: Mapa de inicio en la aplicación

Como vemos en el CPD tenemos alguna incidencia que como máximo es de nivel alta por su color de fondo. Lo vamos a ver mejor en la figura 35 ya

que es el mapa que hace referencia el nodo CPD y en ella vemos como hay alertas de menor nivel como es la de advertencia.

En el mapa del CPD hemos vinculado los 4 grandes grupos que hemos creado para la gestión de ZABBIX en el CPD, Linux producción, Linux desarrollo, Windows producción y Windows desarrollo. Por lo que cualquier error de cada grupo se verá referenciado en su correspondiente nodo y además, si pinchamos en el icono del grupo podremos dirigirnos a un listado de los problemas encontrados. Pues vemos cómo quedaría.

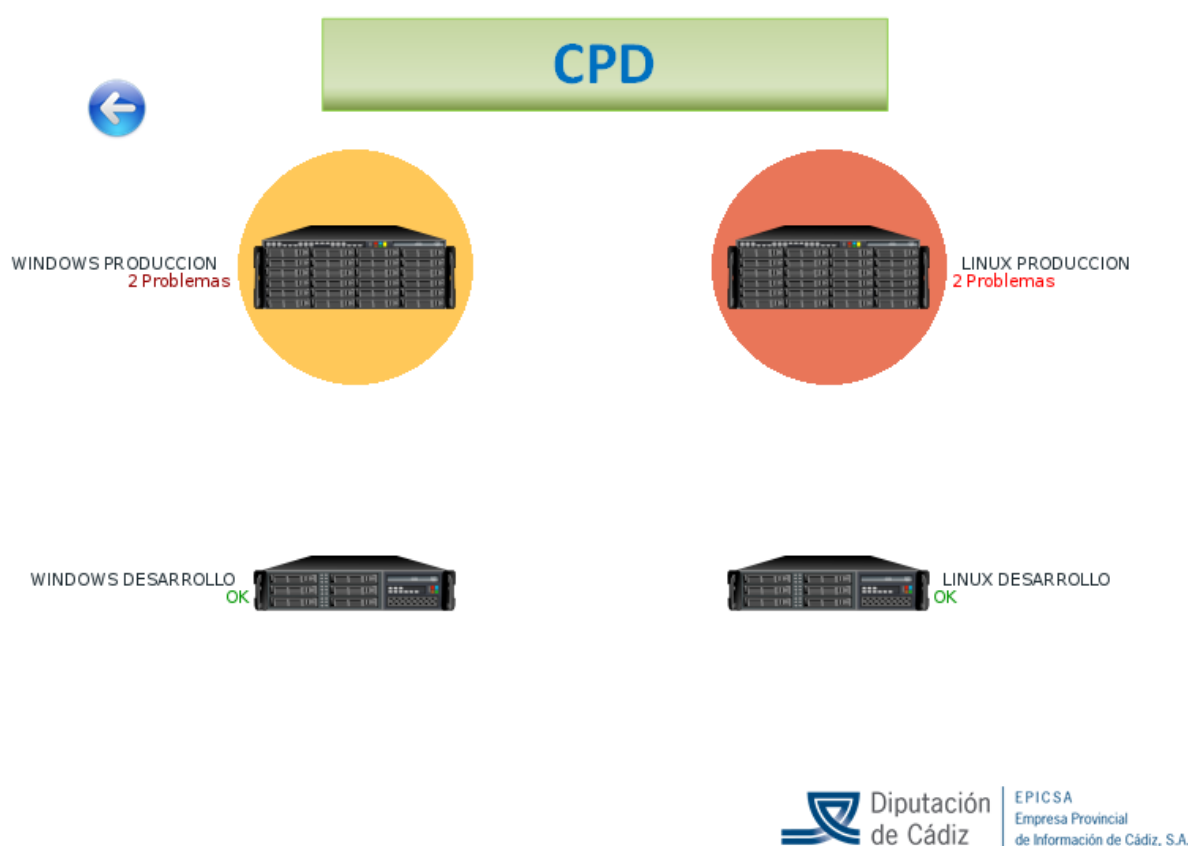


Figura 35: Mapa de grupos CPD

Como vemos ya los 4 problemas que tuvimos en la Figura 34 del nodo del CPD nos la encontramos aquí divididas y ahora veremos cómo nos aparece el listado de los problemas encontrados en el nodo de Windows producción.

<input type="checkbox"/>	GRAVEDAD	ESTADO	INFO	ÚLTIMO CAMBIO ▼	EDAD	ACEPTAR	EQUIPO/PLANTILLA	NOMBRE
<input type="checkbox"/>	Advertencia	PROBLEM		2017-06-30 16:10:35	2d 4h 53m	No 8	OTON3D	Espacio menor del 20% en el volumen E:
<input type="checkbox"/>	Advertencia	PROBLEM		2016-11-25 07:03:34	7m 9d 13h	No 33	OTON3D	Espacio menor del 20% en el volumen C:

Figura 36: Incidencia de Windows producción

A continuación mostraremos como vamos a ver el anillo metropolitano. Este mapa lo hemos creado para ver directamente que es lo que ocurre sin tener que entrar en el edificio ya directamente si una interfaz esta caída nos la indica con los círculos rojo la interfaz que es, y si el conmutador no está operativo nos lo indica cambiando el estado del edificio veamos una ilustración.

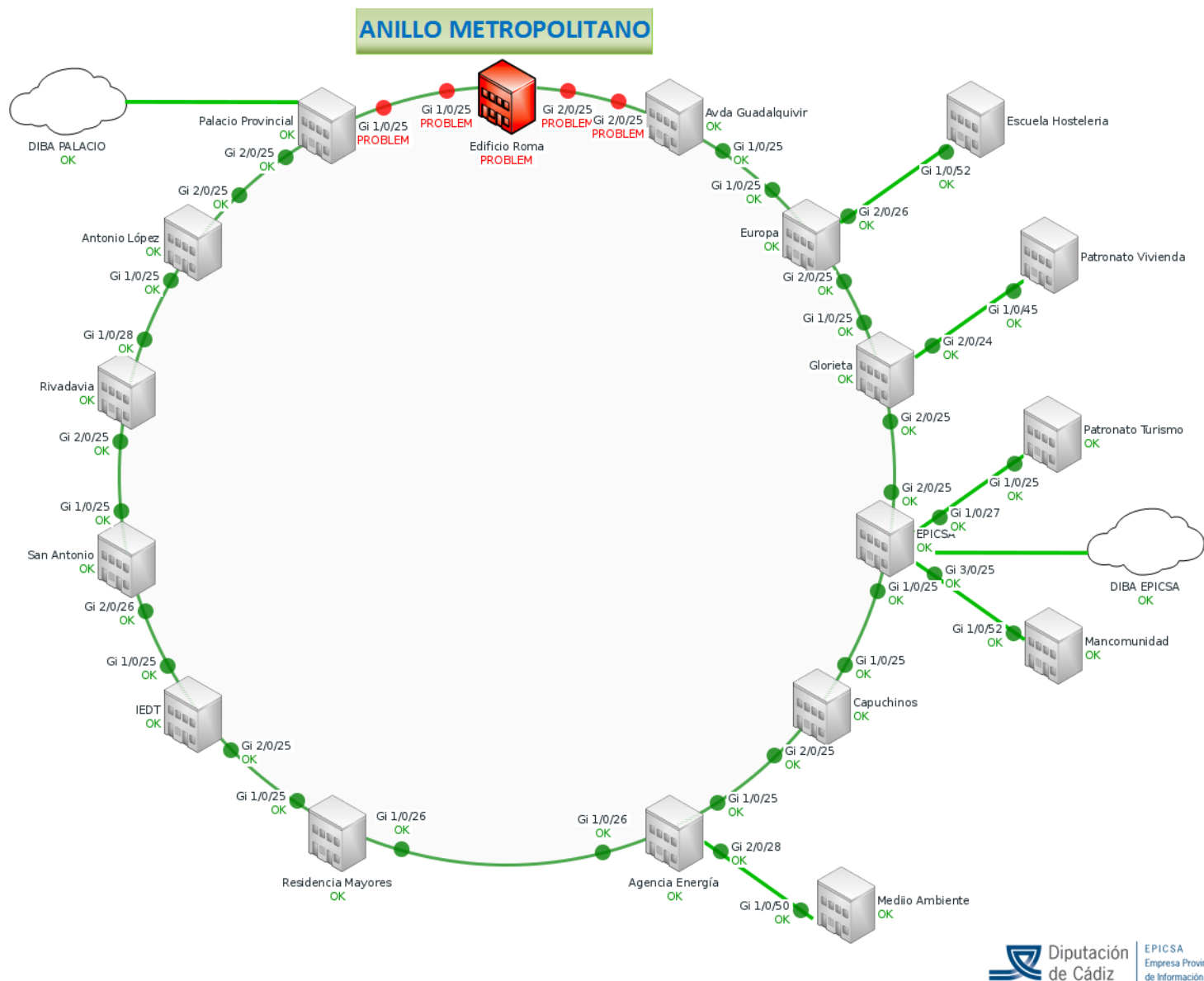


Figura 37: Mapa Anillo Metropolitano

Monitorización de sistemas y redes de la excelentísima diputación provincial de Cádiz

Código: IT5698929

Al igual del mismo modo además de los conmutadores del anillo controlamos los dos accesos a internet que tiene la diputación es decir la DIBA de palacio y la de EPICSA.

Ahora veremos las sedes remotas, para ello vamos a crear un mapa de la provincia de Cádiz, en el que nos indicara si algún ayuntamiento adherido a la diputación de Cádiz tiene algún problema y nos lo indicara con el cambio del punto del ayuntamiento y a la vez podremos acceder al sub mapa de cada ayuntamiento.



Figura 38: Mapa provincial nodos

En caso de algún ayuntamiento tenga algún problema, es decir, se haya iniciado un aviso en el mapa de un ayuntamiento en concreto ese icono cambiará de color. Y para ver qué es lo que está sucediendo entraremos en su submapa para ver que elemento de los que tenemos monitorizado ha fallado.

Los elementos que vamos a indicar en cada mapa de ayuntamiento es el servidor de dominio, el enlace con Epicsa (router VPN) y el medio de acceso a internet (router ADSL) que tengan, lo vemos en la siguiente figura.

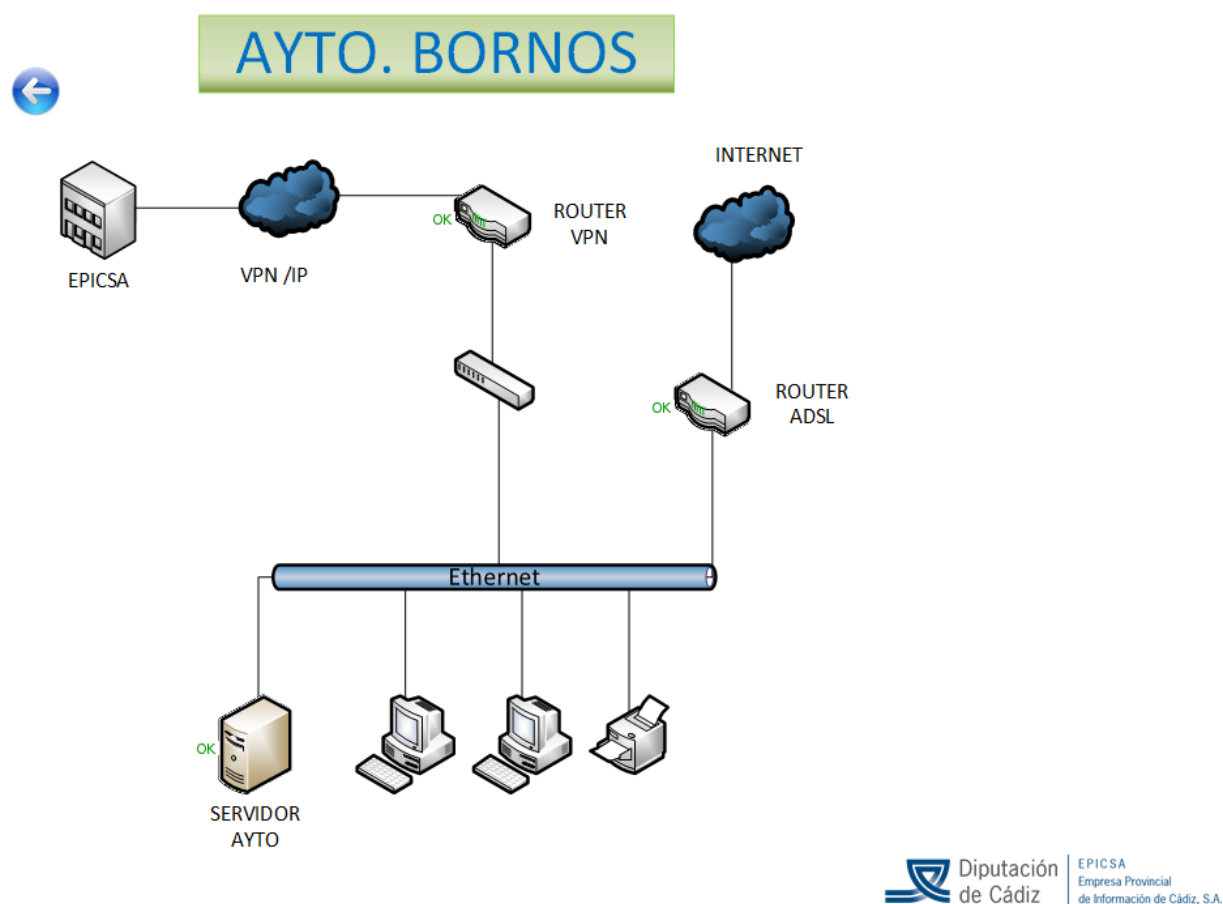


Figura 39: Mapa Ayto. Bornos

1.10. Planificación temporal

Para realización del proyecto se estima que serán necesarias unas 600 horas de trabajo, las cuales, estarán repartidas en un periodo de 4 meses. El comienzo tendrá lugar el 27 de Febrero y su finalización 3 de Julio. Este periodo lo representamos con el siguiente diagrama.

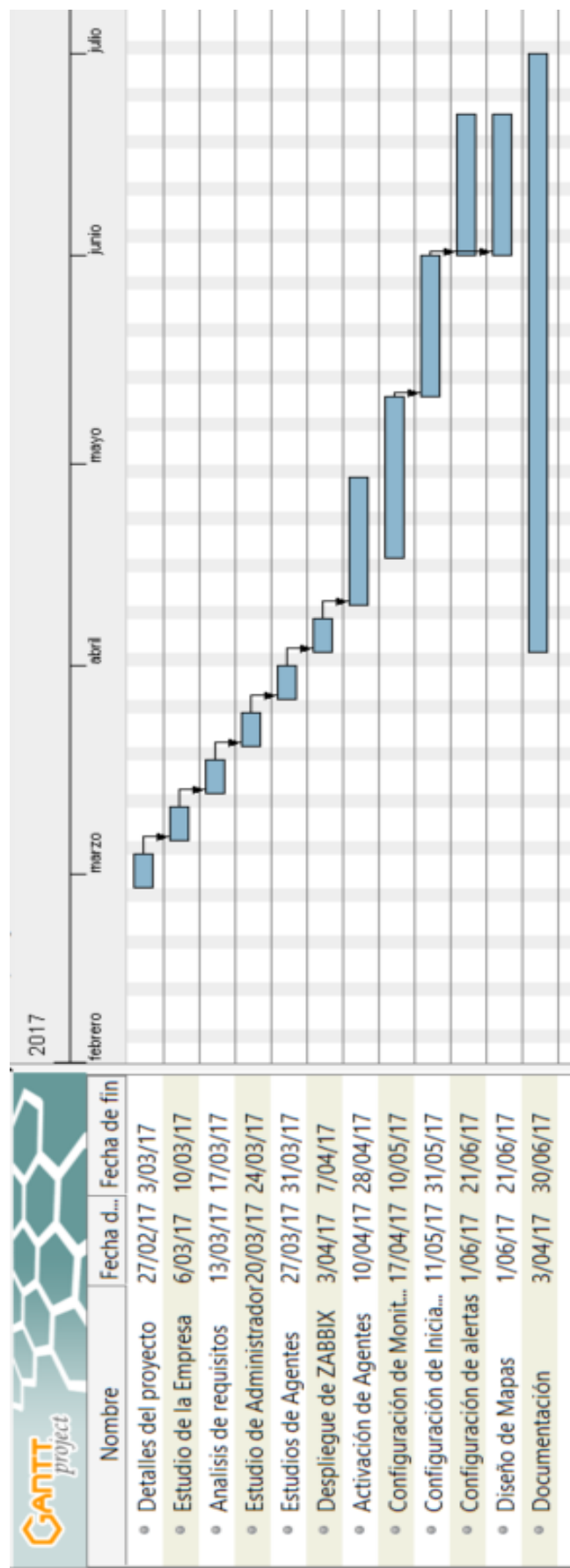


Figura 40: Diagrama de Gantt

1.11. Resumen del presupuesto

Resumen del presupuesto para la realización de la monitorización de gestión de sistemas y redes de la diputación de Cádiz. Para el informe más detallado del presupuesto lo podemos ver en el Capítulo 4 Presupuestos.

Artículos / Servicios	Precio
Blade	6456,32
Telefonía	68,44
Software	0
Mano de Obra	11250
TOTAL	17774,74

Tabla 5: Resumen de Presupuesto

PROYECTO DE MONITORIZACIÓN DE LA GESTION DE SISTEMAS Y REDES DE LA EXCELENTÍSIMA DIPUTACIÓN PROVINCIAL DE CÁDIZ

CÓDIGO: IT5698929

CAPÍTULO 2: ANEXOS

DATOS CLIENTE

EMPRESA PROVINCIAL DE LA INFORMACION DE
CÁDIZ S.A

PLAZA MADRID S/N., EDIFICIO CARRANZA, FONDO
SUR, LOCAL 10,
C.P. 11010 CÁDIZ.

956 26 15 00

DATOS AUTOR

BRAULIO PAREJA MANZANARES

INGENIERO INFORMÁTICO

VIRGEN 5, CONIL, CADIZ
C.P. 11140

BRAULIO.PAREJA.MANZANARES@DIPUCADIZ.ES

FECHA DE PRESENACIÓN

JULIO 2017

FIRMA:

DURACION
ESTIMADA

600 HORAS

BRAULIO PAREJA MANZANARES

2. ANEXOS

A.1 ANEXO 1: Instalación de ZABBIX 3.0

En este momento se ha decidido utilizar la versión 3.0 de Zabbix ya que en su página oficial es la que tiene soporte actualmente, no teniendo aún soporte de instalación su versión más reciente la 3.2. En consecuencia, se ha decidido utilizar la versión 14.04 LTS de Ubuntu ya que es la recomendada para dicha versión de Zabbix. Tras algunas pruebas, parece que la versión más reciente de Ubuntu no es compatible por la versión en la que trabaja el php, pues ésta última versión solo tiene soporte para php7 y Zabbix trabaja con php5.

Instalación de limpia Ubuntu Server lts14.04

- Indicar usuario y contraseña establecidos
- Indicar dirección ip
- Marcar ssh
- Una vez terminada la instalación realizar
 - Sudo apt-get update
 - sudo apt-get upgrade

Instalación de webmin

- antes de instalar Webmin es necesario tener instaladas algunas bibliotecas que webmin usa para funcionar, por eso vamos a instalarlas primero. Uno a uno
 - sudo apt-get install
 - perl
 - libnet-ssleay-perl
 - openssl
 - libauthen-pam-perl
 - libpam-runtime
 - libio-pty-perl
 - apt-show-versions
 - python
 - apache2
- descarga del programa webmin

- wget
http://prdownloads.sourceforge.net/webadmin/webmin_1.801_all.deb
- instalación
 - sudo dpkg --install webmin_1.801_all.deb
- Primer acceso al webmin
 - https://ip_servidor:10000
 - Username
 - Configurado en la instalación de ubuntu
 - Password
 - Configurada en la instalación de ubuntu
 - Configurar idioma
 - Nos dirigimos a
 - [Change Language and Theme](#)
 - Personal choice .. Spanish(ES)
 - Make changes
 - F5
- agregar modulos
 - nos dirigimos a:
 - [Configuración de Webmin](#)
 - Módulos de webmin
 - Módulo estándar de www.webmin.com
 - Phpini
 - Mysql
 - Instalar modulos

Instalación de ZABBIX

- Prerrequisitos, instalación de uno a uno
 - `sudo apt-get install`
 - `mysql-server`
 - Introducir contraseña de root que queremos utilizar

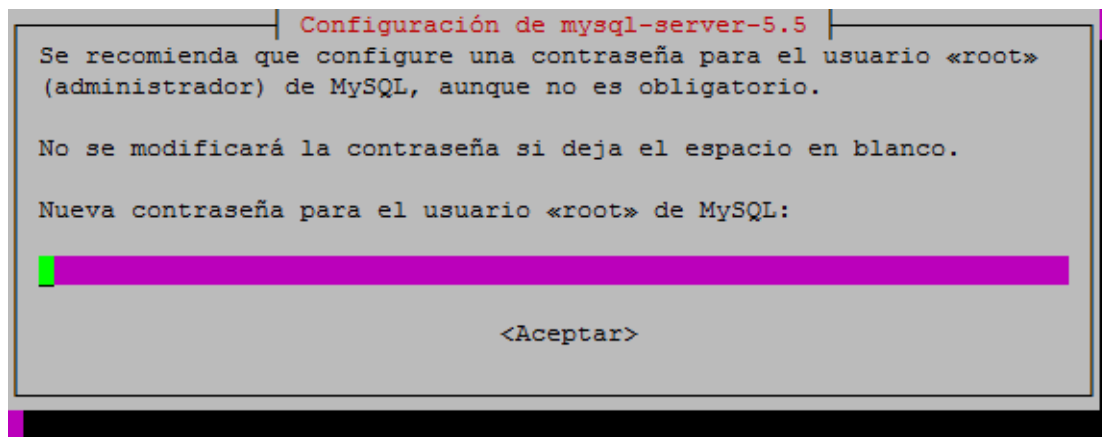


Figura 41: Proceso de instalación Mysql

- `php5`
- `php5-gd` “biblioteca grafica”
- `php-net-socket` “ socket”
- `php5-mysql`
- `php-gettext`
- `php5-ldap`
- *openimi* “controlador de interface de hardware para servidores”
- *libssh2-1*
- *fping*
- `libcurl3` “interprete de comando orientados a la transferencia de archivos”
- *libiksemel3*
- *libxml2*
- `snmp`

- snmpd
- añadir repositorio en `/etc/apt/sources.list` para bcmath
 - `sudo nano /etc/apt/sources.list`
 - añadimos al final del documento la siguiente línea
 - `deb http://us.archive.ubuntu.com/ubuntu`
`xenial main universe`
 - `sudo apt-get update`
 - `php-bcmath`
- *quitar el repositorio anterior añadido en*
`/etc/apt/sources.list`
 - *`sudo nano /etc/apt/sources.list`*
 - *eliminamos la línea*
 - `deb http://us.archive.ubuntu.com/ubuntu`
`xenial main universe`
 - `sudo apt-get update`
- Zabbix paquete
 - `wget`
http://repo.zabbix.com/zabbix/3.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_3.0-1+trusty_all.deb
 - `sudo dpkg -i zabbix-release_3.0-1+trusty_all.deb`
 - `sudo apt-get update`
 - `sudo apt-get install zabbix-server-mysql`
 - `sudo apt-get install zabbix-frontend-php`

- configuración
 - `mysql -uroot -p<password>`
 - `mysql> create database zabbix character set utf8 collate utf8_bin;`
 - `mysql> grant all privileges on zabbix.* to zabbix@localhost identified by '<password>';`
 - `mysql> quit;`
 - `cd /usr/share/doc/zabbix-server-mysql`
 - `zcat create.sql.gz | mysql -uroot zabbix -p`
 - Configurar php
 - Identificamos que los parámetros del siguiente fichero son igual a los valores siguientes mostrados normalmente solo tendremos que des comentar el `php_value date.timezone`
 - `Sudo nano /etc/apache2/conf-enabled/zabbix.conf`

```
<IfModule mod_php5.c>
    php_value max_execution_time 300
    php_value memory_limit 128M
    php_value post_max_size 16M
    php_value upload_max_filesize 2M
    php_value max_input_time 300
    php_value always_populate_raw_post_data -1
    php_value date.timezone Europe/Madrid
</IfModule>
```
 - Configuración del `/etc/zabbix/zabbix_server.conf` añadir los siguientes parámetros
 - `sudo nano /etc/zabbix/zabbix_server.conf`

```
DBHost=localhost
DBName=zabbix
DBUser=zabbix
DBPassword=*****
```
 - `sudo service zabbix-server start`
 - `sudo service apache2 restart`
- Instalación de agente zabbix
 - `sudo apt-get install zabbix-agent`

- Primer acceso a zabbix
 - http://ip_servidor/zabbix/index.php
 - Seguir asistente de instalación



Figura 42: Pantalla bienvenida de Zabbix

- Comprobamos que todos los prerequisites son óptimos es decir que este en **OK**

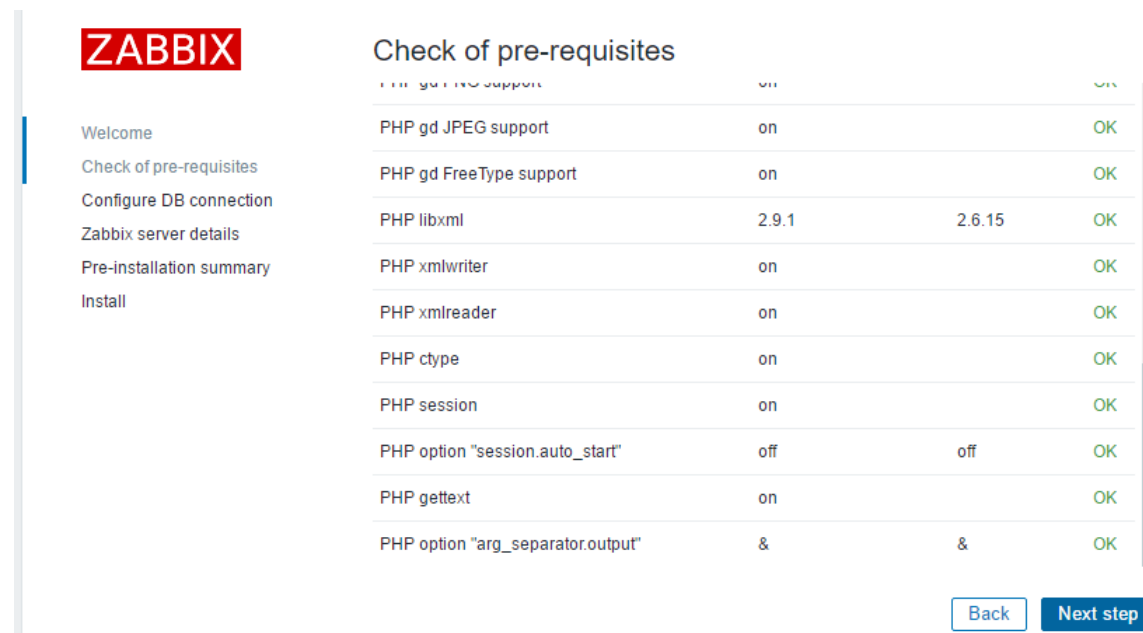


Figura 43: Pantalla de prerequisites

- Introducimos los datos de la base de datos configurada anteriormente

ZABBIX

Welcome
Check of pre-requisites
Configure DB connection
Zabbix server details
Pre-installation summary
Install

Configure DB connection

Please create database manually, and set the configuration parameters for connection to this database. Press "Next step" button when done.

Database type:

Database host:

Database port: 0 - use default port

Database name:

User:

Password:

[Back](#) [Next step](#)

Figura 44: Pantalla de conexión base de datos

- Indicación de parámetros del servidor donde escucha

ZABBIX

Welcome
Check of pre-requisites
Configure DB connection
Zabbix server details
Pre-installation summary
Install

Zabbix server details

Please enter the host name or host IP address and port number of the Zabbix server, as well as the name of the installation (optional).

Host:

Port:

Name:

[Back](#) [Next step](#)

Figura 45: Pantalla de detalles del servidor

- Resumen de los parámetros configurados

ZABBIX

Welcome

Check of pre-requisites

Configure DB connection

Zabbix server details

Pre-installation summary

Install

Pre-installation summary

Please check configuration parameters. If all is correct, press "Next step" button, or "Back" button to change configuration parameters.

Database type	MySQL
Database server	localhost
Database port	default
Database name	zabbix
Database user	zabbix
Database password	*****
Zabbix server	localhost
Zabbix server port	10051
Zabbix server name	

Back Next step

Figura 46: Pantalla de preinstalación

- Ubicación del zabbix frontend

ZABBIX

Welcome

Check of pre-requisites

Configure DB connection

Zabbix server details

Pre-installation summary

Install

Install

Congratulations! You have successfully installed Zabbix frontend.

Configuration file "/usr/share/zabbix/conf/zabbix.conf.php" created.

Back Finish

Figura 47: Pantalla de instalación

- Acceso al portal utilizado usuario y contraseña por defecto de zabbix



The image shows the Zabbix login interface. At the top is the 'ZABBIX' logo in a red box. Below it are two input fields: 'Username' and 'Password'. The 'Username' field contains the character 'l'. Below the password field is a checkbox labeled 'Remember me for 30 days' which is checked. At the bottom is a blue 'Sign in' button. Below the button is a link that says 'or sign in as guest'.

Figura 48: Inicio de sesión

- nos dirigimos a administración – Users
 - elegimos admin
 - y cambiamos el idioma a español
 - si no podemos elegir el idioma deseado realizamos los ‘pasos de configuración de idioma
- Configuración de idioma
 - Primero configuración de los idiomas en el sistema
 - Sudo dpkg-reconfigure locales
 - Para que aparezca el idioma tienes que editar el fichero:
 - Sudo nano /usr/share/zabbix/include/locales.inc.php
 - localizar el idioma que no te aparece y ponerle 'display' a true:
 - 'es_ES' => array('name' => _('Spanish (es_ES)'),
'display' => true),
 - Reiniciamos
 - Sudo service apache2 restart

A.2 ANEXO 2: Instalación de agente ZABBIX en Windows

A continuación, vamos a realizar la instalación del agente en las máquinas con sistema operativo Windows.

- Descargamos de la página oficial de ZABBIX el agente para nuestra versión de ZABBIX
 - http://www.zabbix.com/downloads/3.0.0/zabbix_agents_3.0.0.win.zip
- Extraemos su contenido en c:\zabbix si no existe la carpeta la creamos en la cual contendremos ahora:
 - Bin
 - Conf
- Elegimos un editor de texto y modificamos el archivo localizado en C:\zabbix\conf\zabbix\agentd.win.conf
 - Indicando los siguientes parametros

```
LogFile=c:\zabbix\zabbix_agentd.log
Server=ip_servidor_zabbix
ServerActive= ip_servidor_zabbix
Hostname=Nombre que le queremos dar al equipo a
monitorizar
```

- Una vez configurado el archivo tendremos que instalar el servicio para ello nos dirigimos al símbolo de sistema de Windows ejecutándolo como administrador
 - Inicio
 - Cmd
 - Botón derecho ejecutar como administrador
- En la consola nos desplazamos a la versión de Windows que tengamos 32 o 64 en nuestro caso 64 en la carpeta descomprimida anteriormente de zabbix.
 - Cd c:\zabbix\bin\win64
- Procedemos a instalar el agente con nuestras configuraciones anteriores a través del siguiente comando
 - c:\zabbix\bin\win64>zabbix_agentd.exe --config
c:\zabbix\conf\zabbix_agentd.win.conf --install

⁴ «Zabbix Manual [Zabbix Documentation 3.0]».

A.3 ANEXO 3: instalación de agente ZABBIX en Debian / Ubuntu

A continuación, vamos a realizar la instalación del agente en las máquinas con sistema operativo Ubuntu

- Descargamos el repositorio oficial para poder realizar la instalación
 - Wget
http://repo.zabbix.com/zabbix/3.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_3.0-1+trusty_all.deb
 - `sudo dpkg -i zabbix-release_3.0-1+trusty_all.deb`
 - `sudo apt-get update`
- A continuación instalamos el agente
 - `sudo apt-get install zabbix-agent`
- Realizamos ahora la configuración del agente por lo que modificamos el siguiente archivo `zabbix_agentd.conf`
 - `Sudo nano /etc/zabbix/zabbix_agentd.conf`
 - Indicamos los siguientes parámetros

```
LogFile=c:\zabbix\zabbix_agentd.log

Server=ip_servidor_zabbix
ServerActive= ip_servidor_zabbix
Hostname=Nombre que le queremos dar al equipo a
monitorizar
```
- Una vez configurado el archivo tendremos que iniciar el servicio
 - `Sudo /etc/init.d/zabbix-agent restart`

A.4 ANEXO 4: Configuración de SNMP en equipos Windows

Ahora vamos a configurar el servicio SNMP para los equipos Windows. Según la versión puede variar un poco, pero normalmente, los pasos son los que se indican a continuación.

Tenemos que tener claro la comunidad en la que vamos a añadir los equipos y el equipo que puede pedir las peticiones, ya que tendremos que indicarlo a lo largo del proceso; así como, la versión de SNMP que vamos a utilizar en principio. Solo vamos a utilizar la versión 2 por el tema de compatibilidad.

- Inicio
 - Panel de control
 - Programas y características
 - Activar o desactivar características de Windows
 - Aquí buscamos la característica que queremos activar:
 - Protocolo simple de administración de redes(SNMP)

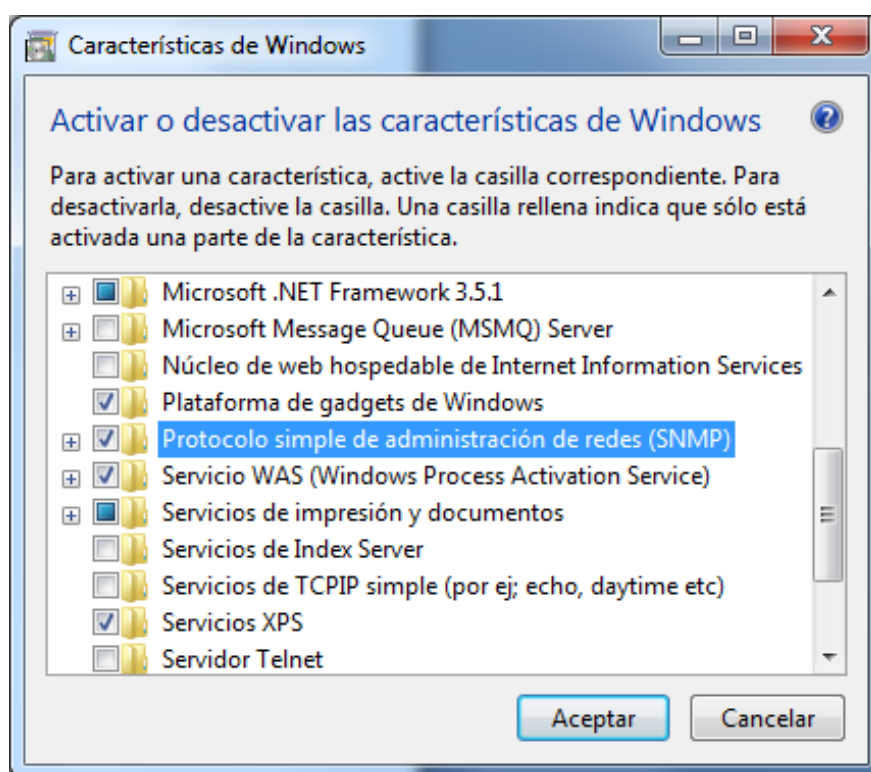


Figura 49: Activar SNMP característica

- Ahora nos dirigimos a configurar el servicio
 - Inicio y tecleamos servicios
 - En el panel de servicios locales buscamos servicio SNMP
 - Propiedades
 - Y realizamos las siguientes acciones:
 - Captura
 - Agregamos el nombre de la comunidad y el destino

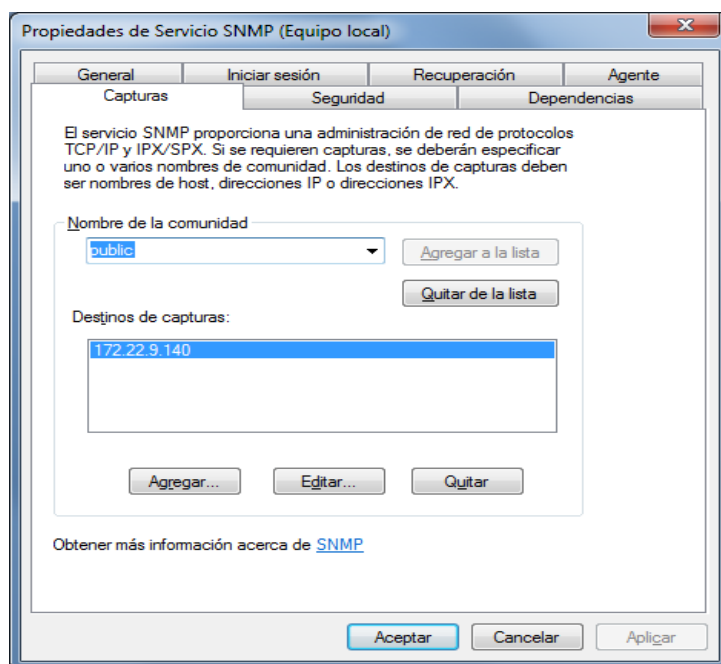


Figura 50: Propiedades de servicio SNMP Capturas

- seguridad
 - Agregamos la comunidad y los permisos deseados
 - Aceptar paquetes deseados desde cualquier host

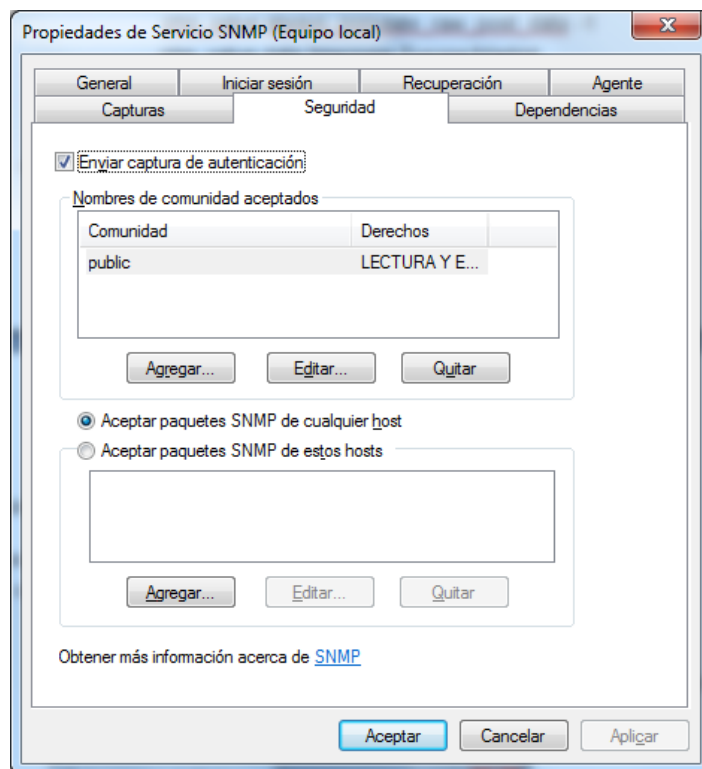


Figura 51: Propiedades de servicio SNMP Seguridad

- Agente

- Marcamos todas las opciones

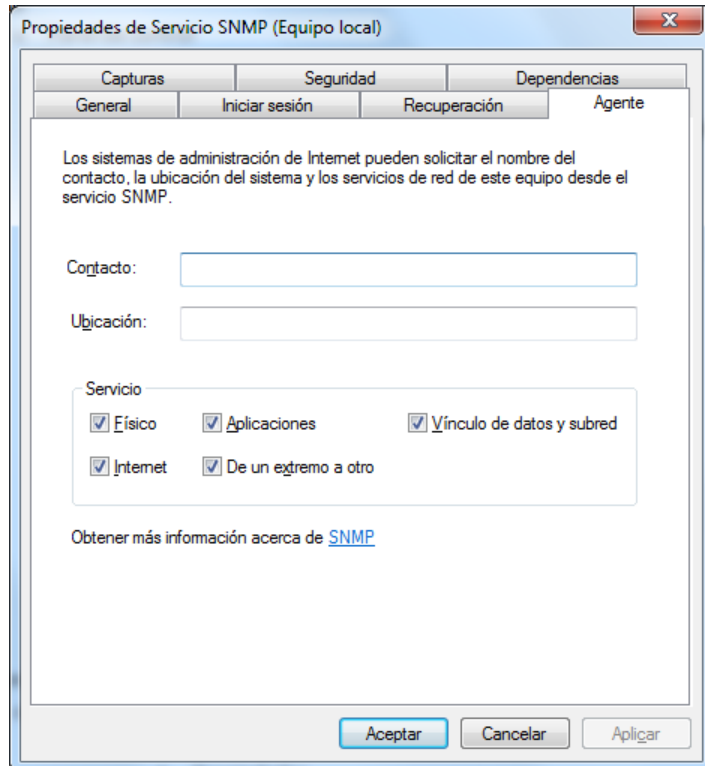


Figura 52: Propiedades de servicio SNMP Agente

Comprobamos que todo lo realizado ha salido bien. Para ello nos dirigiremos a un equipo con la instalación de `snmpd` bajo Linux y realizamos el siguiente comando que nos dirá el nombre del equipo:

- `snmpget -M MIBs -c public -v 1 10.12.100.62 .1.3.6.1.2.1.1.5.0`

Lo que realizamos es una petición a la máquina para comprobar que está activo el servicio SNMP y el cual nos contesta con el nombre de la máquina.

A.5 ANEXO 5: Conexión modem NOKIA TM-1

Para poder realizar envío de SMS con el ZABBIX es necesario la configuración de un modem con sim. Para ello disponemos en la empresa del modem NOKIA TM-1, para el cual se ha realizado los siguientes pasos para su instalación en el sistema operativo que tenemos alojado nuestro servicio de monitorización, es decir, en Ubuntu Server 14.04 LTS.

En principio, se ha tenido problemas a la hora de configurar el equipo para mandar SMS ya que hemos utilizado un conversor de usb a serial para poder establecer conexión con el modem GSM.

Después de las pruebas, tenemos que utilizar un cable serie directo para establecer conexión los parámetros de configuración serian:

Bps: 9600

Bit de datos: 8

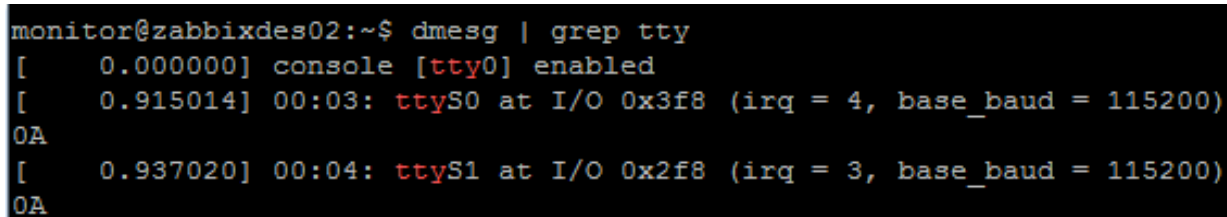
Paridad: Ninguno

Bits de Parada: 1

Control de flujo: Hardware

Antes de realizar las pruebas con Zabbix, lo primero que tenemos que hacer es, ver qué puertos están activos. Para ello introducimos el siguiente comando:

- `dmesg | grep tty`



```
monitor@zabbixdes02:~$ dmesg | grep tty
[ 0.000000] console [tty0] enabled
[ 0.915014] 00:03: ttyS0 at I/O 0x3f8 (irq = 4, base_baud = 115200)
0A
[ 0.937020] 00:04: ttyS1 at I/O 0x2f8 (irq = 3, base_baud = 115200)
0A
```

Figura 53: Puertos activos tty

En nuestro caso hemos conectado el modem al COM 1 por lo tanto utilizamos ttyS0 al ver que está ya enabled.

A continuación, tenemos que configurar el modem para su correcto funcionamiento y para ello instalamos minicom para dar los parámetros al modem y guardarlos.

Lo instalamos con el siguiente comando:

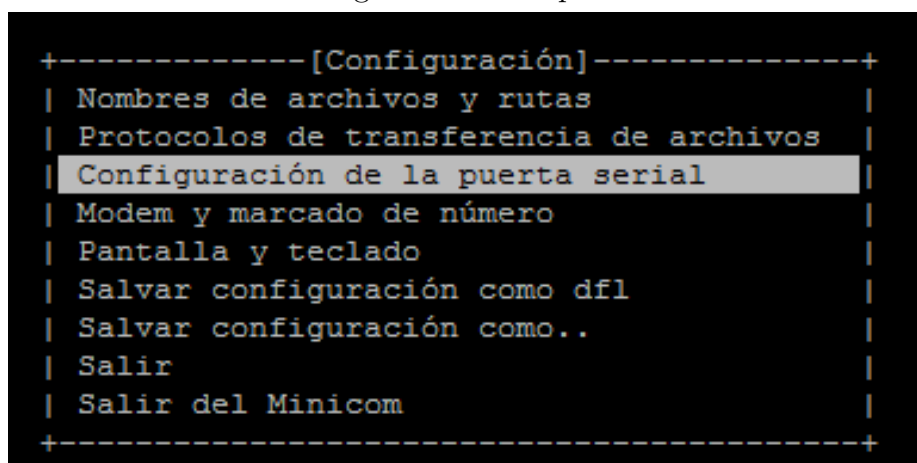
- Sudo apt-get install minicom

Luego ejecutamos el programa para poder configurar la conexión.

- Sudo minicom -s

Para su correcto funcionamiento iremos realizando los siguientes pasos:

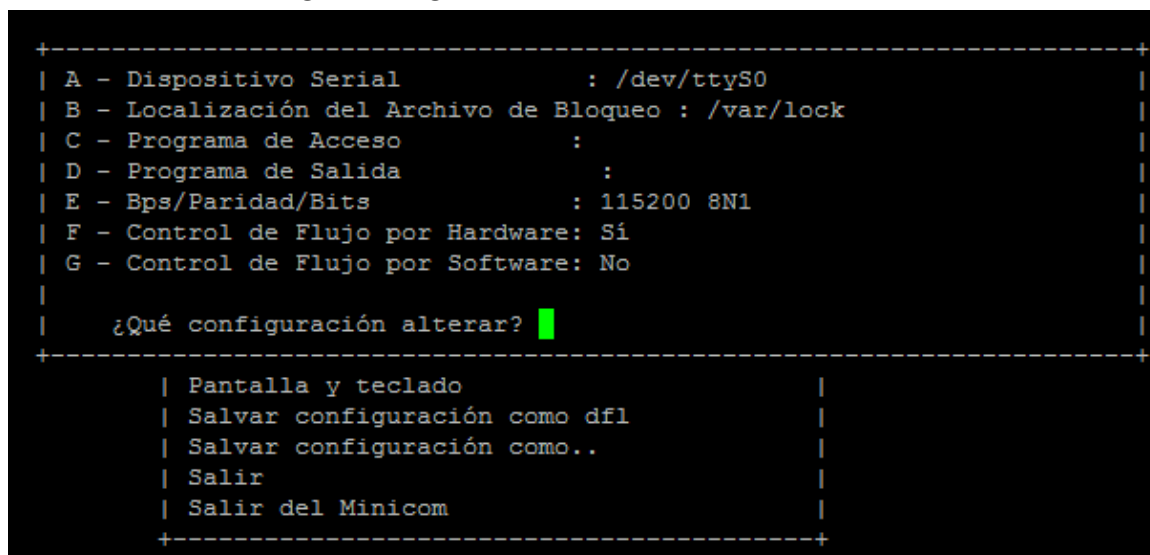
- Ahora nos vamos a configuración de la puerta serial



```
+-----[Configuración]-----+
| Nombres de archivos y rutas |
| Protocolos de transferencia de archivos |
| Configuración de la puerta serial |
| Modem y marcado de número |
| Pantalla y teclado |
| Salvar configuración como dfl |
| Salvar configuración como.. |
| Salir |
| Salir del Minicom |
+-----+
```

Figura 54: Minicom puerta serial

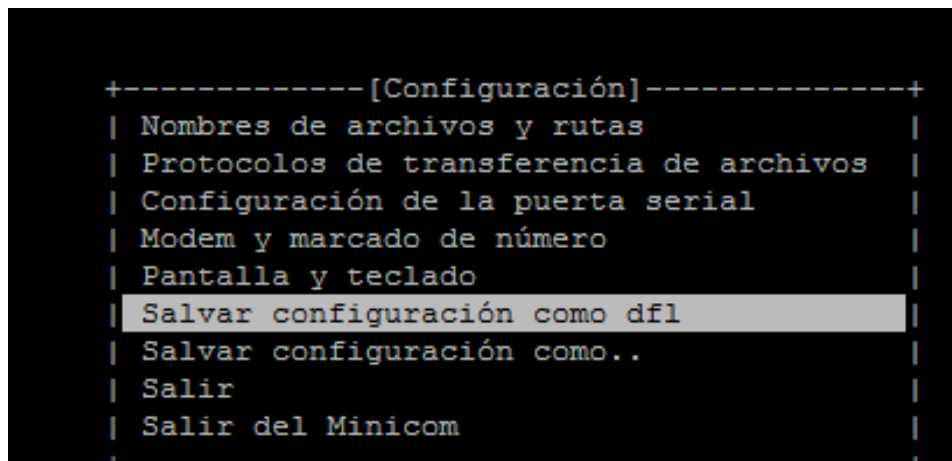
- Indicamos los parámetros de configuración de nuestro modem que lo vemos en la siguiente figura.



```
+-----+
| A - Dispositivo Serial      : /dev/ttyS0 |
| B - Localización del Archivo de Bloqueo : /var/lock |
| C - Programa de Acceso     : |
| D - Programa de Salida     : |
| E - Bps/Paridad/Bits       : 115200 8N1 |
| F - Control de Flujo por Hardware: Sí |
| G - Control de Flujo por Software: No |
| |
| ¿Qué configuración alterar? █ |
+-----+
| Pantalla y teclado |
| Salvar configuración como dfl |
| Salvar configuración como.. |
| Salir |
| Salir del Minicom |
+-----+
```

Figura 55: Minicom parametros

- Para finalizar salvamos la configuración como dfl y salimos del programa



```

+-----[Configuración]-----+
| Nombres de archivos y rutas |
| Protocolos de transferencia de archivos |
| Configuración de la puerta serial |
| Modem y marcado de número |
| Pantalla y teclado |
| Salvar configuración como dfl |
| Salvar configuración como.. |
| Salir |
| Salir del Minicom |
+-----+

```

Figura 56: Minicom salvar dfl

Para verificar que lo que hemos realizado está bien, entramos en la consola en la que pondremos los siguientes parámetros:

- At
Ok
- At+cpin="XXXX" (Pin de la sim)
OK
- At+cmgf=1
Ok
- ctrl+a q (para salir de la consola ya que todo nos ha confirmado ok)

Una vez terminado con el programa minicom aún no hemos finalizado, ya que esta configuración cada que vez que se reinicie el sistema se pierde, por lo que vamos a instalar el software WVDIAL para que guarde la configuración al cargar. Lo realizamos con los siguientes comandos:

- Sudo apt-get install wvdial (Su instalación)
- sudo wvdialconf (Ejecución)
 - para que guarde la configuración actual en /etc/wvdial.conf.

A continuación añadimos estas 2 líneas al fichero anterior

- [Dialer pin]
- Init1 = AT+CPIN="XXXX"

Para finalizar los pasos previos Agregamos el usuario zabbix al grupo de usuario dialout del sistema

Ya solo nos queda configurara el modulo SMS en ZABBIX.

A.6 ANEXO 6: Activación SNMP FORTIGATE 800C

Vamos a realizar la configuración del firewall Fortigate para la activación el servicio snmp v2. Para ello tenemos que entrar en el portal web y logarnos como administrador y a continuación realizar los siguientes pasos:

- Nos dirigimos ha sistema y a continuación SNMP
- Pinchamos en crear Nuevo
 - Introducimos el nombre de la comunidad
 - En Hosts
 - Indicamos desde la dirección o conjunto de direcciones que van a poder realizar consultas de snmp

FortiGate 800C FG800C3913802642

Nueva Comunidad

Nombre de Comunidad

Hosts:

Dirección IP/Máscara	Tipo de Host	Eliminar
<input type="text" value="direccion ip del servidor zabbix"/>	<input type="text" value="Aceptar consultas y enviar notificaciones"/>	

Agregar

Consultas:

Protocolo	Puerto
v1	<input type="text" value="161"/>
v2c	<input type="text" value="161"/>

Traps:

Protocolo	Local	Remoto
v1	<input type="text" value="162"/>	<input type="text" value="162"/>
v2c	<input type="text" value="162"/>	<input type="text" value="162"/>

Evento SNMP

<input checked="" type="checkbox"/> Utilización de CPU es alta	<input checked="" type="checkbox"/> Memoria es baja
<input checked="" type="checkbox"/> Poco espacio en Disco para Log	<input checked="" type="checkbox"/> IP de Interface ha cambiado
<input checked="" type="checkbox"/> Túnel de VPN arriba	<input checked="" type="checkbox"/> Túnel de VPN abajo
<input checked="" type="checkbox"/> WiFi Controller AP arriba	<input checked="" type="checkbox"/> WiFi Controller AP abajo
<input checked="" type="checkbox"/> Sesión FortiSwitch Controller arriba	<input checked="" type="checkbox"/> Sesión FortiSwitch Controller abajo
<input checked="" type="checkbox"/> Estado de Clúster de HA ha cambiado	<input checked="" type="checkbox"/> Falla en el HA heartbeat
<input checked="" type="checkbox"/> Miembro HA arriba	<input checked="" type="checkbox"/> Miembro HA abajo
<input checked="" type="checkbox"/> Virus detectado	<input checked="" type="checkbox"/> Patrón de Archivo Detectado

Figura 57: Fortigate Datos Comunidad

- En Eventos SNMP elegimos que eventos podemos monitorizar.

A.7 ANEXO 7: Activación SNMP HP-5500

En este anexo, vamos a realizar la activación de SNMP en los conmutadores HP-5500 para ello en primer lugar tenemos que autenticarnos su plataforma web:

- Una vez autenticados nos dirigimos al apartado de la derecha QoS
 - Entramos en ACL IPv4
 - Si ya tenemos una ACL activa lo único que haremos es agregar una nueva regla en la que añadiremos la dirección IP del administrador ZABBIX. Para ello vamos a Basic Setup y elegimos la ACL a la que le vamos a agregar la regla.

Figura 58: Añadir Regla Acl HP5500

- En caso que no tengamos la ACL la creamos dándole a add y a continuación realizamos los pasos anteriores y aplicamos

Figura 59: Crear ACL HP5500

- Para finalizar nos dirigimos al menú principal a:
 - Device , luego SNMP
 - Una vez aquí agregamos la comunidad que tenemos en común con el servidor y además añadir la ACL anteriormente creada y para ello nos vamos a community.

Setup Community Group User Trap View

Add SNMP Community

Community Name *(1-32Chars.)

Access Right

View

ACL (2000-2999)

Items marked with an asterisk(*) are required

Apply Cancel

Figura 60: Comunidad HP5500

- Para finalizar activamos la versión de SNMP que vamos a utilizar en la pestaña Setup y aplicamos

Setup Community Group User Trap View

SNMP ☒ Enable ☐ Disable

Local Engine ID *(10-64 Hex Chars.)

Maximum Packet Size *Bytes(484-17940, Default = 1500)

Contact (1-255Chars.)

Location (1-255Chars.)

SNMP Version ☐ v1 ☒ v2c ☒ v3

Note: If you disable SNMP, all SNMP related configurations will not be saved.

Items marked with an asterisk(*) are required

Apply Cancel

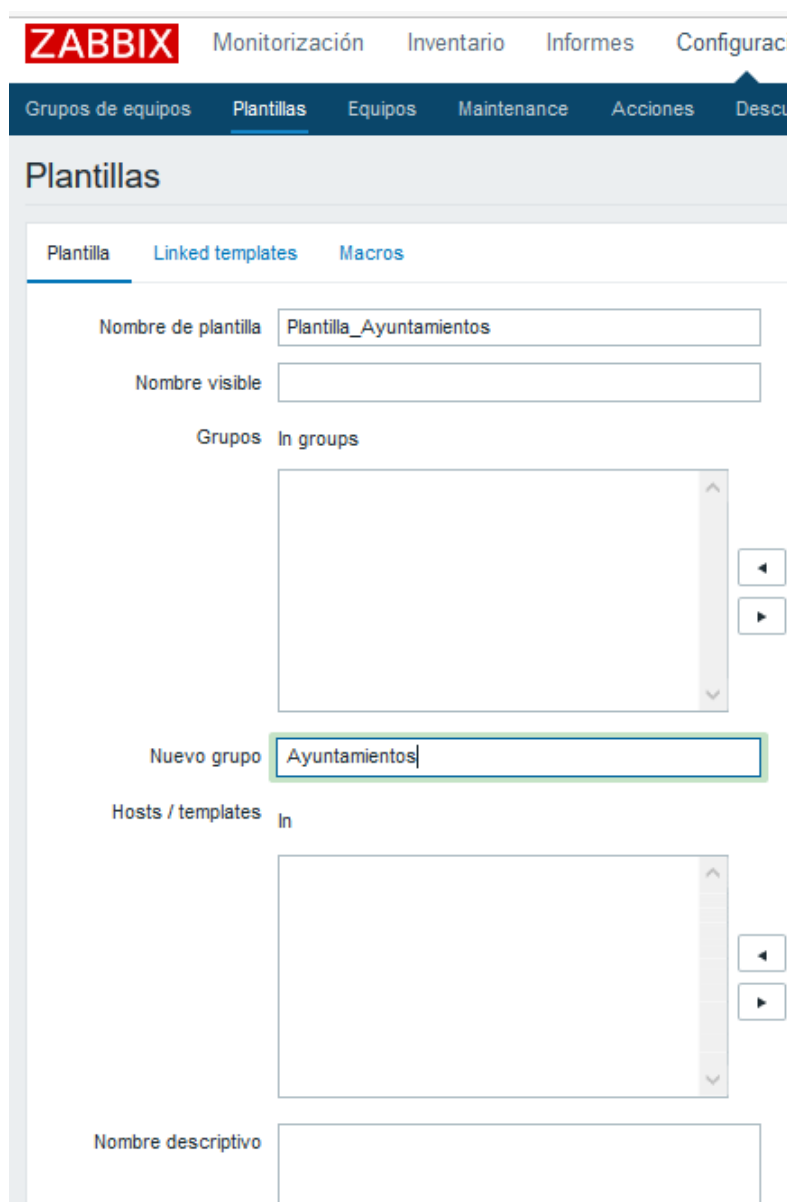
Figura 61: Activa SNMP HP5500

No podemos olvidarnos de salvar la configuración en el apartado Device - configuration, ya que si el conmutador se reinicia perderemos la configuración.

A.8 ANEXO 8: Configuración de Plantilla en ZABBIX

En este apartado vamos a ver como se configura una plantilla para equipos en ZABBIX, en la que tendremos que crear monitores, iniciadores y gráficos.

En primer lugar nos dirigimos a Configuración – Plantillas – Crear plantilla aquí introducimos el nombre de la plantilla y creamos o seleccionamos un nuevo grupo. E incluso si queremos podemos añadir ya plantillas anteriormente creada

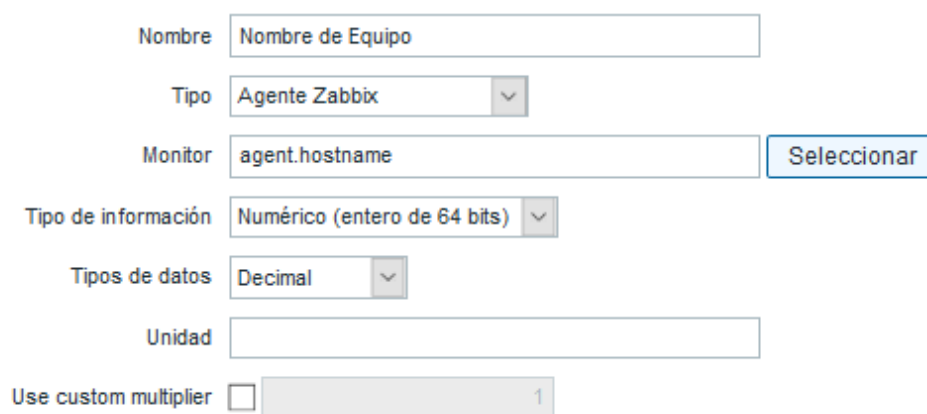


The screenshot shows the Zabbix web interface for creating a new template. The top navigation bar includes 'Monitorización', 'Inventario', 'Informes', and 'Configuración'. The left sidebar has 'Grupos de equipos', 'Plantillas', 'Equipos', 'Maintenance', 'Acciones', and 'Descu'. The main content area is titled 'Plantillas' and has tabs for 'Plantilla', 'Linked templates', and 'Macros'. The 'Plantilla' tab is active, showing a form with the following fields: 'Nombre de plantilla' (filled with 'Plantilla_Ayuntamientos'), 'Nombre visible' (empty), 'Grupos' (a list box with 'In groups' and empty space, and navigation buttons), 'Nuevo grupo' (filled with 'Ayuntamientos' and highlighted with a green border), 'Hosts / templates' (a list box with 'In' and empty space, and navigation buttons), and 'Nombre descriptivo' (empty).

Figura 62: Crear plantilla zabbix

A continuación le damos a agregar y buscamos la plantilla creada para empezar a crear monitores. Nos dirigimos a la pestaña Monitores y luego Crear Monitor. En primer lugar, le indicamos el nombre que queremos darle. Luego tenemos que indicar que tipo de agente elegir. Llegado a éste punto, vamos a trabajar con 3 opciones como ya hemos dicho en la memoria, para ello tendríamos que seleccionar en el campo tipo: Agente ZABBIX, Agente SNMP V2 o Comprobación sencilla. Si elegimos Agente ZABBIX podremos seleccionar un monitor de la opción que nos aparece en seleccionar y le pondríamos los parámetros que fueran necesarios al igual que comprobación sencilla. Pero si seleccionamos agente SNMP, se complica un poco más, pues tendríamos que saber el OID del elemento que queremos monitorizar. Y para ello tendremos que tener las MIBS del fabricante. Vamos a ver un ejemplo de cada opción.

En primer lugar vemos en la imagen un monitor de agente Zabbix

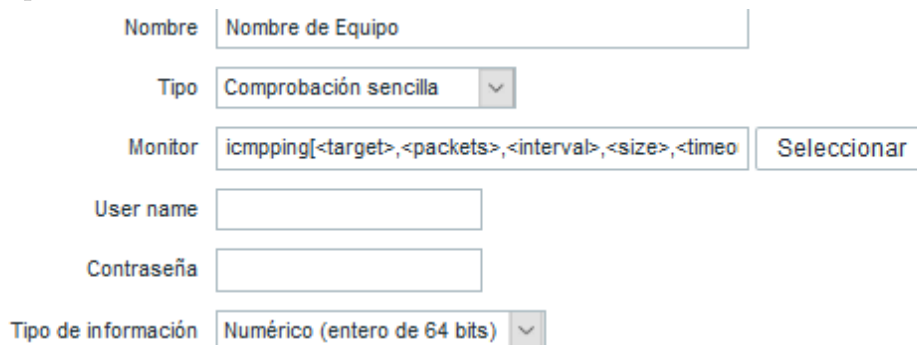


Formulario de creación de monitor para Agente Zabbix. El formulario contiene los siguientes campos:

- Nombre:** Campo de texto con el valor "Nombre de Equipo".
- Tipo:** Selector de lista desplegable con el valor "Agente Zabbix".
- Monitor:** Campo de texto con el valor "agent.hostname" y un botón "Seleccionar" a su derecha.
- Tipo de información:** Selector de lista desplegable con el valor "Numérico (entero de 64 bits)".
- Tipos de datos:** Selector de lista desplegable con el valor "Decimal".
- Unidad:** Campo de texto vacío.
- Use custom multiplier:** Casilla de verificación desactivada y un campo de texto con el valor "1".

Figura 63: Creación Monitor Agente ZABBIX

Al seleccionar el monitor del combo no tendríamos que indicar que tipo de información contiene el monitor ni qué tipo de datos ya que estos campos obtienen el tipo al seleccionarlo. Al igual pasa con la siguiente ilustración de comprobación sencilla



Formulario de creación de monitor para Comprobación sencilla. El formulario contiene los siguientes campos:

- Nombre:** Campo de texto con el valor "Nombre de Equipo".
- Tipo:** Selector de lista desplegable con el valor "Comprobación sencilla".
- Monitor:** Campo de texto con el valor "icmping[<target>,<packets>,<interval>,<size>,<timeo" y un botón "Seleccionar" a su derecha.
- User name:** Campo de texto vacío.
- Contraseña:** Campo de texto vacío.
- Tipo de información:** Selector de lista desplegable con el valor "Numérico (entero de 64 bits)".

Figura 64: Creación de Monitor Comprobación sencilla

Ahora veremos la última opción de monitor que nos parecerá más difícil al principio, pero, sabiendo navegar bien por las bibliotecas de MIBS no tendríamos problemas. Pero eso sí, tendremos que saber también el tipo de información que nos devuelve el monitor para así poder representarlo. En este caso es de tipo registro

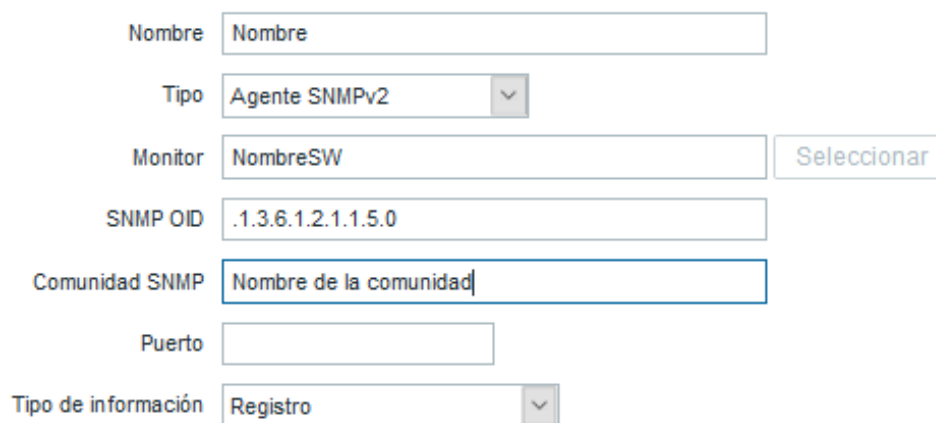
El formulario muestra los campos para configurar un monitor SNMP. Los campos son: 'Nombre' con el valor 'Nombre', 'Tipo' con un menú desplegable que muestra 'Agente SNMPv2', 'Monitor' con el valor 'NombreSW' y un botón 'Seleccionar' a su derecha, 'SNMP OID' con el valor '.1.3.6.1.2.1.1.5.0', 'Comunidad SNMP' con el valor 'Nombre de la comunidad', 'Puerto' vacío, y 'Tipo de información' con un menú desplegable que muestra 'Registro'.

Figura 65: Creación de Monitor SNMP

La ilustración de la figura 65 es un monitor que lo que vamos a obtener es el nombre de un conmutador HP5500 a través de su OID. Este en particular utilizar la biblioteca pública de MIB-2 como vemos en la estructura del árbol que se muestra a continuación

[1.3.6.1.2.1.1.5](#) - sysName

[1.3.6.1.2.1.1](#) - SNMP MIB-2 System

[1.3.6.1.2.1](#) - SNMP MIB-2

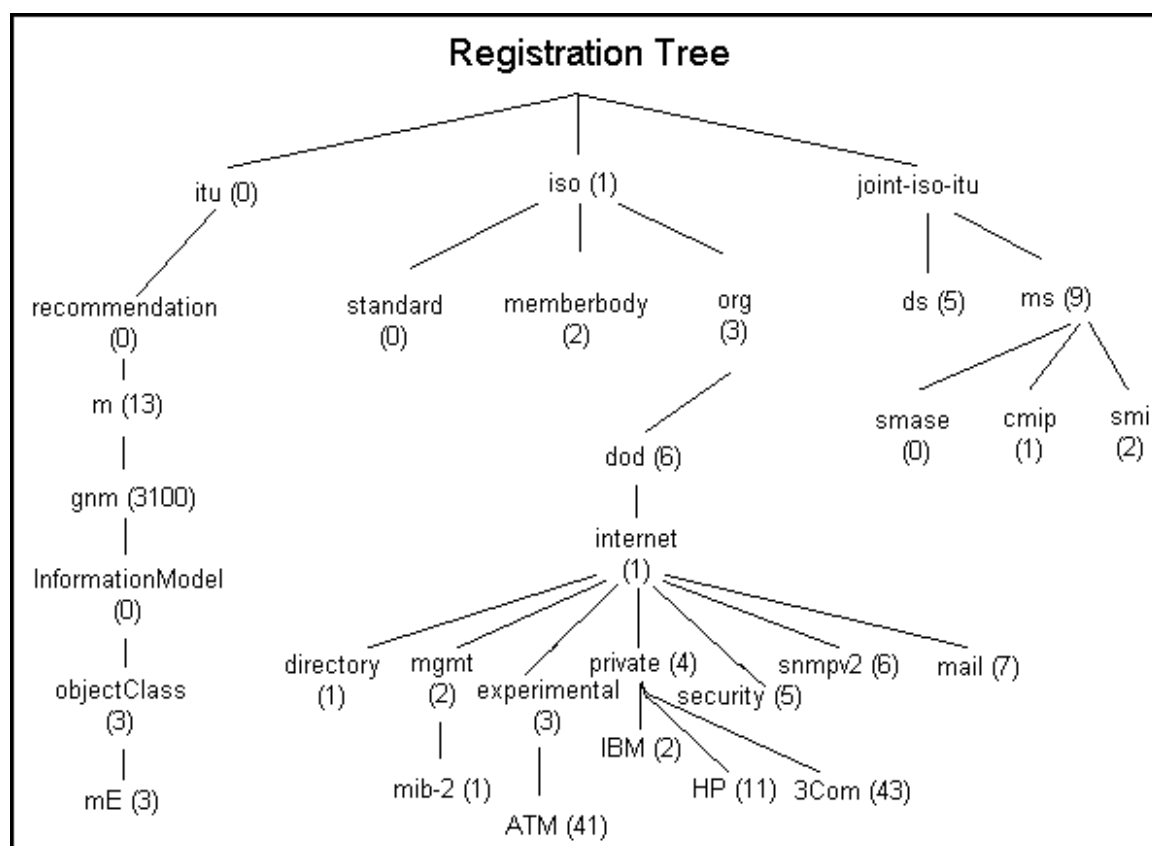
[1.3.6.1.2](#) - MGMT Management

[1.3.6.1](#) - Internet assignments from 1.3.6.1

[1.3.6](#) - DOD Department of Defense

[1.3](#) - ORG Identified Organization

[1](#) - ISO assigned OIDs

Figura 66; Árbol de estructura MIB General⁵

Ya elegido el monitor a utilizar, los siguientes pasos son iguales para todos los monitores. Tenemos que asignar un intervalo de actualización, es decir cada cuanto tiempo queremos que compruebe el valor del monitor. Aquí podremos decidir entre varias opciones e incluso por una fecha determinada.

Intervalo de actualización (en segundos)

Intervalos personalizados

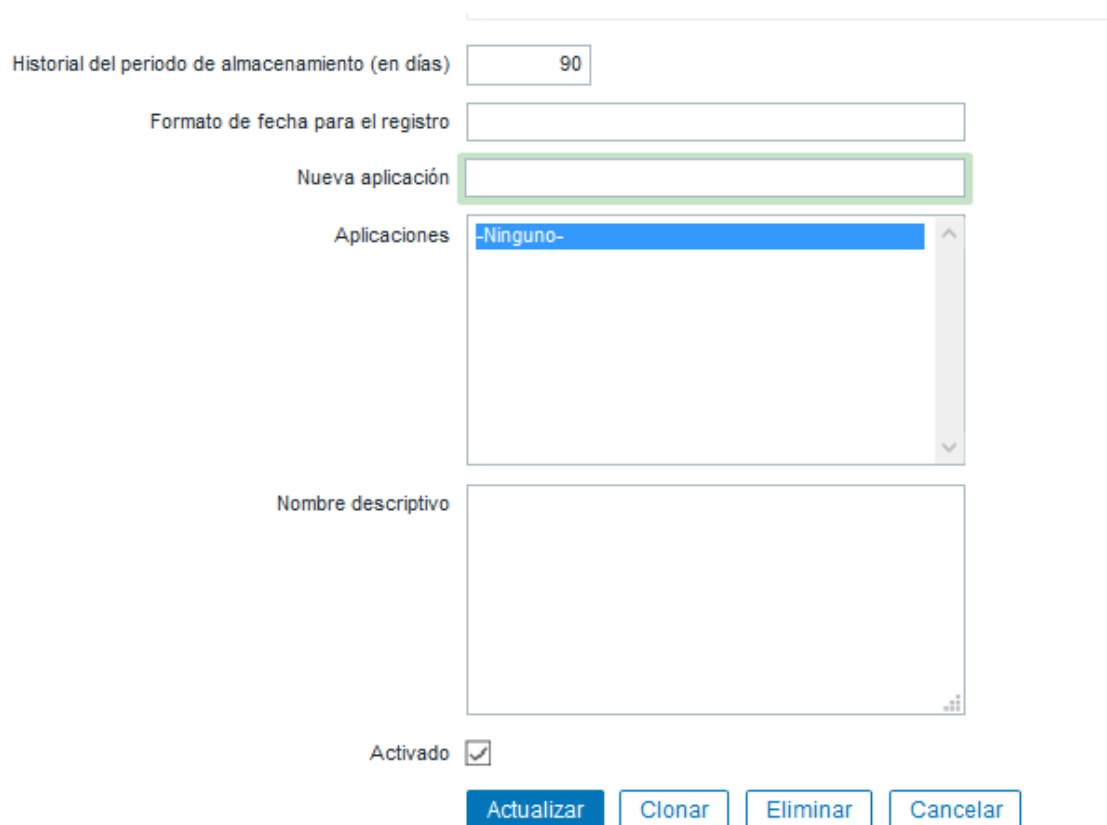
TIPO	INTERVAL	PERÍODO
Flexible	Scheduling	50
		1-7,00:00-

[Agregar](#)

Figura 67: Intervalos de un Monitor

También podremos decidir qué tiempo de registro queremos que guarde los valores que vamos obteniendo así como su formato de fecha. Y para finalizar, podremos añadir una aplicación o elegir una ya existente para esta plantilla. Realmente la utilidad que tiene es para organizar un poco mejor los monitores en grupos pero solo cobra sentido si tiene una gran cantidad de ellos.

⁵ «Submodelo de información en OSI».



Formulario de configuración del Monitor:

- Historial del periodo de almacenamiento (en días):
- Formato de fecha para el registro:
- Nueva aplicación:
- Aplicaciones:
 - Ninguno-
- Nombre descriptivo:
- Activado: ☒
- Botones:

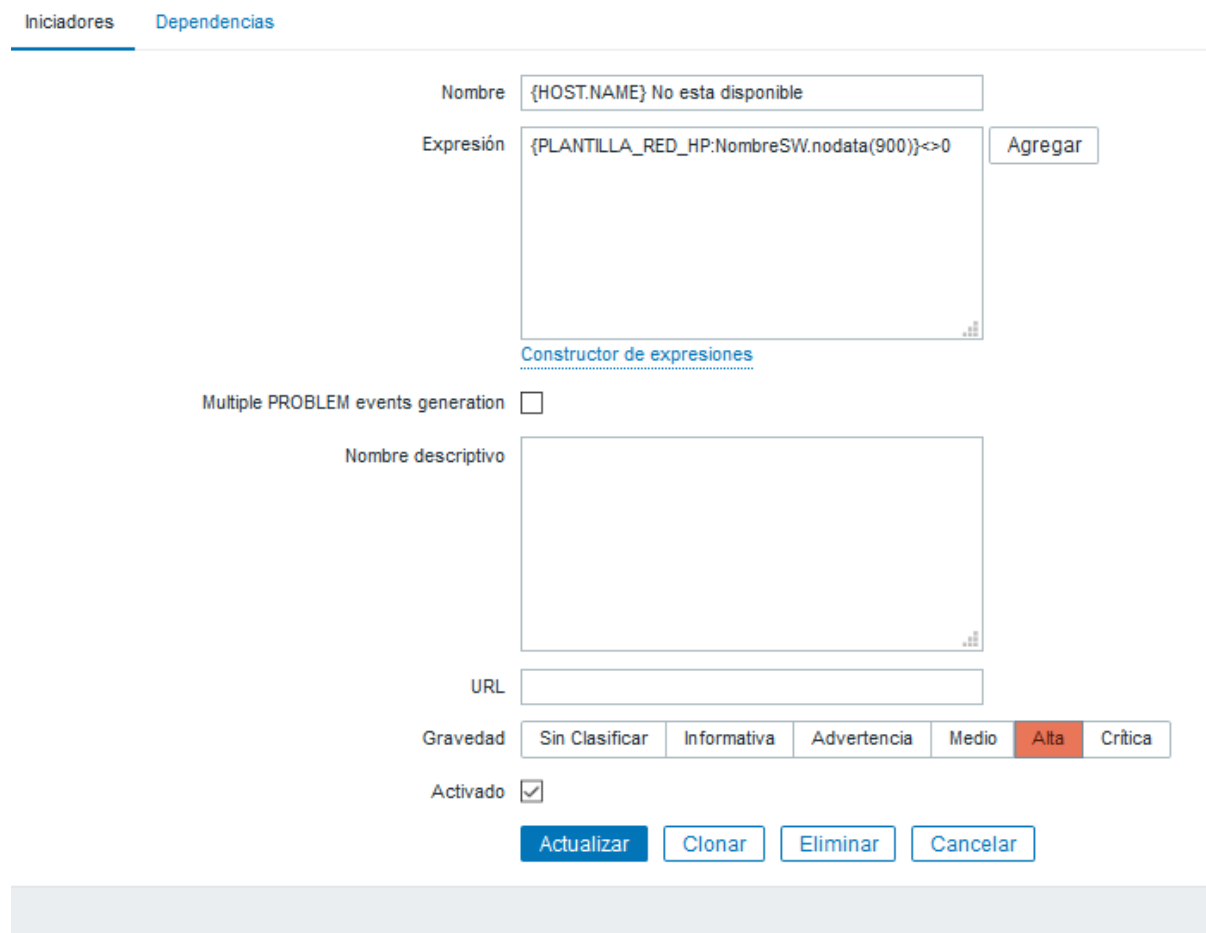
Figura 68: Periodo de almacenamiento del Monitor

Muy importante pinchar en actualizar ya que si no podríamos perder los cambios.

Ya con nuestro monitor creado nos disponemos a crear un iniciador, que lo que hace es alertarnos de que el monitor no está obteniendo un valor esperado. Nos dirigimos a la opción iniciador y pinchamos en crear iniciador. Una vez aquí, le indicamos el nombre con el que queremos que nos aparezca y construimos la expresión sobre el monitor que queramos.

Por ejemplo en la Figura 69, lo que vamos a realizar es un indicador para cuando no recibamos datos que nos avise que el sistema no se encuentra disponible por ello después del nombre del monitor ponemos `nodata(900)<>0` lo que nos indica es que si dentro de 15 minutos mi valor es distinto a 0 es este caso 1 ya que 1 es que no tiene valor el monitor, entonces me iniciaré. Para realizarlo hemos jugado con los tiempos de actualización del monitor, ya que para este monitor tenemos un refresco cada 10 minutos así que en el peor de los casos sabremos que hemos tenido un corte en la red pasado unos 15 minutos.

Una opción que tenemos que tener en cuenta en el iniciador es indicarle que grado de gravedad contiene, para así poder tener una mejor organización y filtrar para la ejecución de acciones



Dependencias

Nombre {HOST.NAME} No esta disponible

Expresión {PLANTILLA_RED_HP:NombreSW.nodata(900)}<=>0 Agregar

Constructor de expresiones

Multiple PROBLEM events generation ☐

Nombre descriptivo

URL

Gravedad Sin Clasificar Informativa Advertencia Medio **Alta** Crítica

Activado ☒

Actualizar Clonar Eliminar Cancelar

Figura 69: Creación de iniciador

Para finalizar vamos a crear un gráfico. Es bastante sencillo, pues lo único que se tiene que saber es qué monitor se va a utilizar para generar el gráfico. Nos dirigimos a la opción gráficos y picamos en crear gráfico, una vez aquí tan solo tenemos que poner el nombre, elegir el tipo de gráfico y seleccionar que monitor o monitores sobre los que se va a realizar al gráfico.

Una vez que sabemos realizar estas acciones con las plantillas, si queremos realizar un monitor determinado para un equipo o cualquier otro componente de los que hemos visto se realizará del mismo modo pero en el equipo.

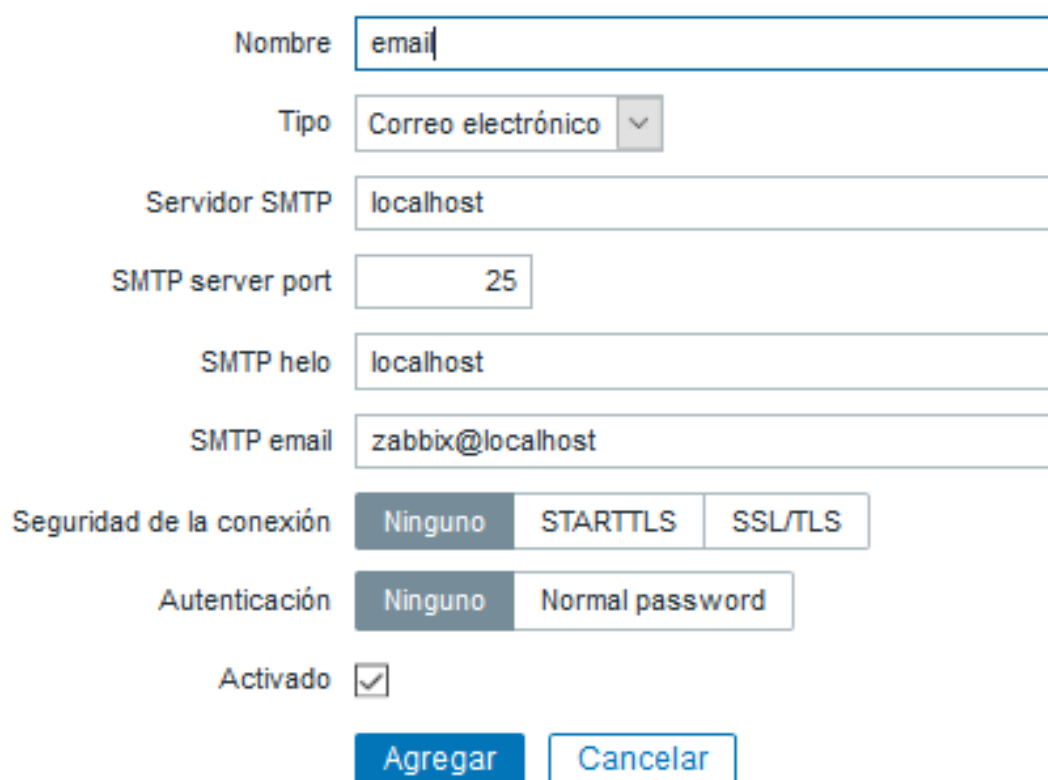
A.9 ANEXO 9: Configuración de tipos de medios

ZABBIX

En esta sección vamos a configurar los medios por los que los administradores pueden ser alertados.

A.9.1 E-mail configuración

Para activar este medio nos dirigimos a administración – tipos de medio y elegimos email, Configuramos los parámetros de nuestro servidor de correo



The image shows a web form for configuring an email media type in Zabbix. The form includes the following fields and options:

- Nombre:** A text input field containing the value "email".
- Tipo:** A dropdown menu with "Correo electrónico" selected.
- Servidor SMTP:** A text input field containing "localhost".
- SMTP server port:** A text input field containing "25".
- SMTP helo:** A text input field containing "localhost".
- SMTP email:** A text input field containing "zabbix@localhost".
- Seguridad de la conexión:** A group of three buttons: "Ninguno" (selected), "STARTTLS", and "SSL/TLS".
- Autenticación:** A group of two buttons: "Ninguno" (selected) and "Normal password".
- Activado:** A checkbox that is checked.
- Buttons:** Two buttons at the bottom, "Agregar" (Add) and "Cancelar" (Cancel).

Figura 70: Crear medio Email

Una vez configurado, le indicaremos el correo al usuario para ello nos dirigimos a administración – Usuarios – agregar.

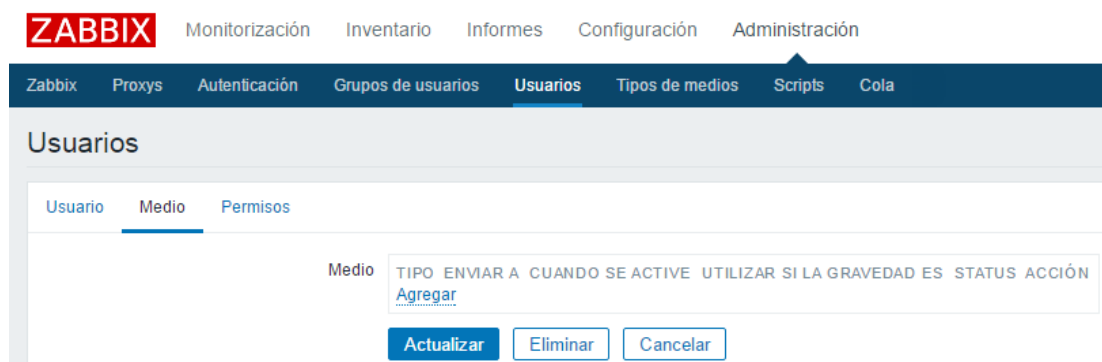


Figura 71: Medio de usuario

Elegimos el tipo de medio en este caso email o el nombre que le demos cuando agregamos el nuevo tipo de medio anteriormente. Escribimos el email del usuario y agregamos.

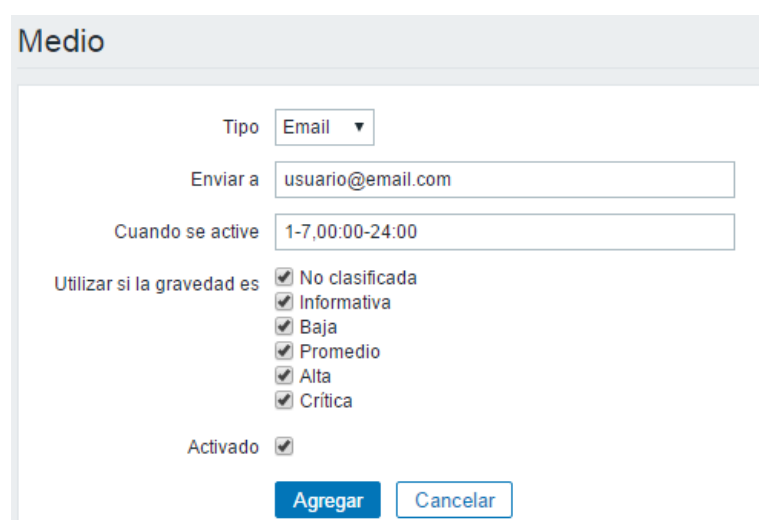


Figura 72: Especificación de medio Email

Y por último nos dirigimos a configuración – acciones. Creamos una nueva o editamos alguna existente, vamos a operaciones -- nuevo. Agregamos los usuario a quien queremos que envía la notificación y elegimos el medio por el que queremos transmitir en nuestro caso Email.

The screenshot shows the ZABBIX 'Acciones' (Actions) configuration page. The 'Operaciones' (Operations) tab is selected. The 'Duración predeterminada del paso de operación' (Default operation step duration) is set to 3600 seconds. The 'PASOS DETALLES' (Step details) section shows a single step with the action 'Send message to users: Braulio (Braulio), Manolo (Manolo) via Email Immediately Por defecto'. The 'Operation details' section shows the step duration set to 0, the operation to perform is 'Enviar mensaje', and the 'Send to User groups' is 'UN GRUPO DE USUARIOS'. The 'Enviar a usuarios' (Send to users) table lists 'Braulio (Braulio)' and 'Manolo (Manolo)' with 'Eliminar' (Delete) links. The 'Send only to' is set to 'Email', and the 'Mensaje por defecto' (Default message) checkbox is checked. The 'Condiciones' (Conditions) section shows a condition 'Nuevo' (New) with an 'Agregar' (Add) link. At the bottom, there are buttons for 'Actualizar' (Update), 'Clonar' (Clone), 'Eliminar' (Delete), and 'Cancelar' (Cancel).

Figura 73: Operaciones con email

A.9.2. Jabber configuración

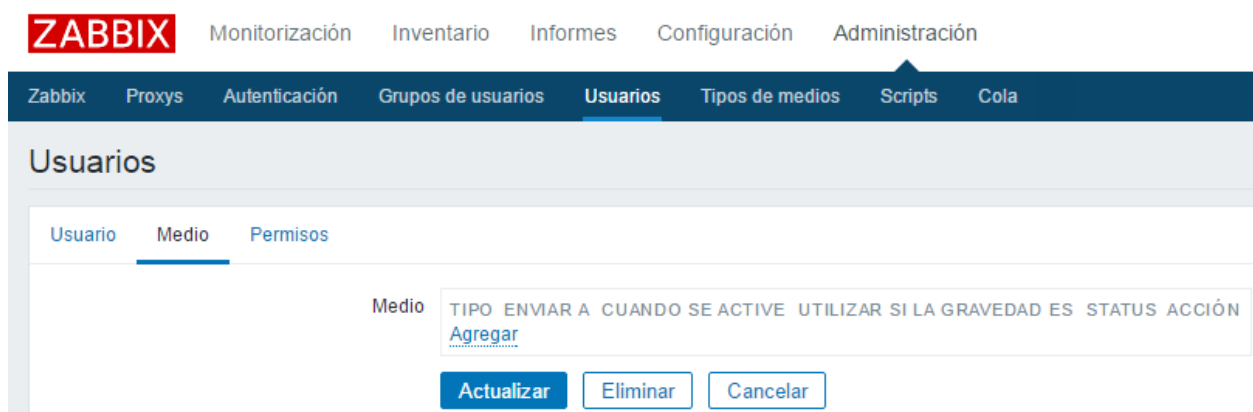
Aunque de momento no vamos a utilizar la mensajería instantánea, vamos a dejarlo configurado.

Nos dirigimos a administración – tipos de medio y elegimos Jabber, Configuramos los parámetros de nuestro usuario

The screenshot shows the ZABBIX 'Tipos de medios' (Media types) configuration page. The 'Tipos de medios' tab is selected. The 'Nombre' (Name) field is set to 'Jabber'. The 'Tipo' (Type) dropdown is set to 'Jabber'. The 'Identificador Jabber' (Jabber identifier) field is set to 'zabbix@zabbixdes02'. The 'Contraseña' (Password) field has a 'Cambiar la contraseña' (Change password) button. The 'Activado' (Activated) checkbox is checked. At the bottom, there are buttons for 'Actualizar' (Update), 'Clonar' (Clone), 'Eliminar' (Delete), and 'Cancelar' (Cancel).

Figura 74: Crear medio jabber

Una vez configurado, le indicaremos el correo al usuario para ello nos dirigimos a administración – usuario – agregar



ZABBIX Monitorización Inventario Informes Configuración Administración

Zabbix Proxys Autenticación Grupos de usuarios **Usuarios** Tipos de medios Scripts Cola

Usuarios

Usuario Medio **Permisos**

Medio

TIPO	ENVIAR A	CUANDO SE ACTIVE	UTILIZAR SI LA GRAVEDAD ES	STATUS	ACCIÓN
Agregar					

[Actualizar](#) [Eliminar](#) [Cancelar](#)

Figura 75: Alta de Jabber en usuario

Elegimos el tipo de medio en este caso Jabber el nombre que le demos cuando agregamos el nuevo tipo de medio anteriormente. Escribimos el usuario de jabber y agregamos.



Medio

Tipo **Jabber**

Enviar a **usuario@jabber**

Cuando se active **1-7,00:00-24:00**

Utilizar si la gravedad es

- ☒ No clasificada
- ☒ Informativa
- ☒ Baja
- ☒ Promedio
- ☒ Alta
- ☒ Crítica

Activado ☒

[Agregar](#) [Cancelar](#)

Figura 76: Asignación usuario Jabber

Y por último nos dirigimos a configuración – acciones. Creamos una nueva o editamos alguna existente, vamos a operaciones -- nuevo. Agregamos los usuario o grupo a quien queremos que envía la notificación y elegimos el medio por el que queremos transmitir en nuestro mensaje en este caso usuario jabber.

The screenshot displays the Zabbix configuration interface for actions, specifically the 'Operaciones' (Operations) tab. The interface shows settings for a step duration of 3600 seconds. Under 'Operaciones de la acción', step 1 is 'Send message to user groups: Zabbix administrators via Jabber' with a start time of 'Immediate'. The 'Operation details' section shows 1 step, 0 duration, and the action 'Enviar mensaje'. It lists 'Zabbix administrators' as a user group with an 'Agregar' button. There is also a 'Enviar a usuarios' section with an 'Agregar' button. The 'Send only to' dropdown is set to 'Jabber'. A 'Mensaje por defecto' checkbox is checked. At the bottom, there are buttons for 'Actualizar', 'Clonar', 'Eliminar', and 'Cancelar'.

Figura 77: Asignación de operaciones al usuario jabber

A9.3. SMS Configuración

Por ultimo realizaremos la configuración de envío de mensajería simple.

Nos dirigimos a administración – tipos de medio y elegimos SMS, Indicamos el modem GSM donde está conectado.

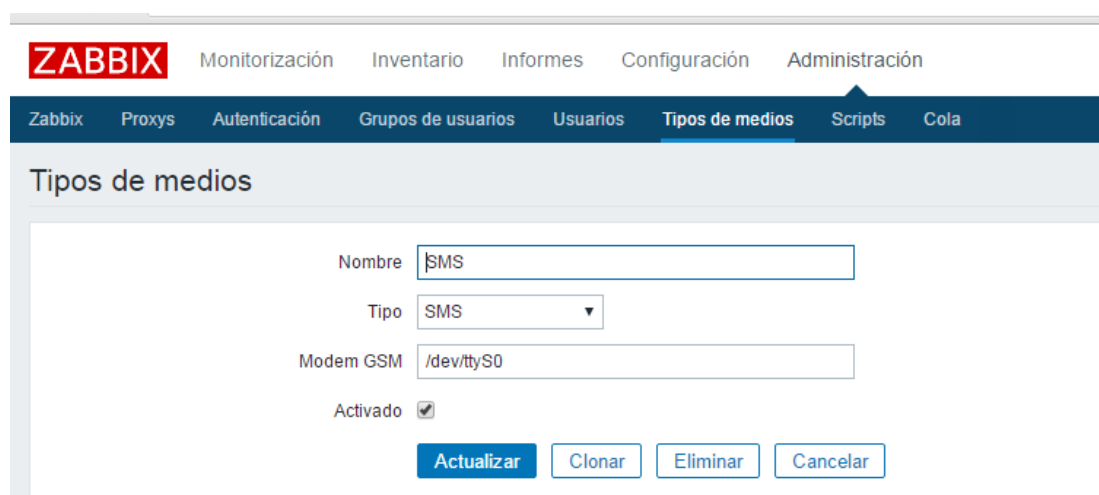


Figura 78: Crear medio SMS

Una vez configurado, le indicaremos el correo al usuario para ello nos dirigimos a administración – usuario – agregar

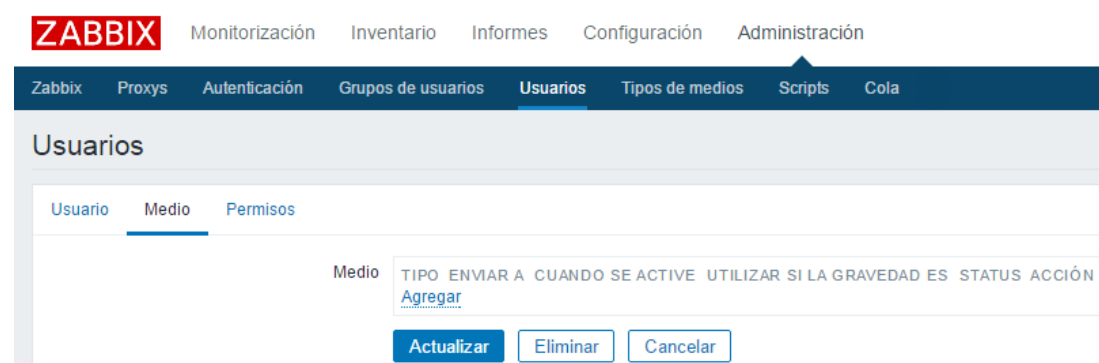


Figura 79: Alta de SMS en usuario

Elegimos el tipo de medio en este caso SMS o el nombre que le demos cuando agregamos el nuevo tipo de medio anteriormente. Escribimos el teléfono del usuario y agregamos

Tipo **SMS**

Enviar a **+3466666666**

Cuando se active **1-7,00:00-24:00**

Utilizar si la gravedad es

- ☒ No clasificada
- ☒ Informativa
- ☒ Baja
- ☒ Promedio
- ☒ Alta
- ☒ Crítica

Activado ☒

Actualizar **Cancelar**

Figura 80: Asignación de teléfono al usuario

Y por último nos dirigimos a configuración – acciones. Creamos una nueva o editamos alguna existente, vamos a operaciones -- nuevo. Agregamos los usuario a quien queremos que envía la notificación y elegimos el medio por el que queremos transmitir en nuestro caso SMS. Tenemos que tener en cuenta que al ser mensaje de texto no debemos pasar de 160 caracteres.

Acciones

Acción Condiciones Operaciones

Duración predeterminada del paso de operación **3600** (minimum 60 seconds)

Operaciones de la acción

PASOS	DETALLES	START IN	DURACIÓN (s)
1	Send message to users: Braulio (Braulio) via SMS	Immediately	Por defecto

[Nuevo](#)

Actualizar **Clonar** **Eliminar** **Cancelar**

Figura 81: Asignación de operación para usuario SMS

A partir de aquí, también podemos generar acciones a realizar en el equipo que estemos monitoreando siempre y cuando se permitan. Tenemos varias opciones a elegir para poder realizar comandos remotos.

PROYECTO DE MONITORIZACIÓN DE LA GESTION DE SISTEMAS Y REDES DE LA EXCELENTÍSIMA DIPUTACIÓN PROVINCIAL DE CÁDIZ

CÓDIGO: IT5698929

CAPÍTULO 3: ESPECIFICACIONES DEL SISTEMA

DATOS CLIENTE

EMPRESA PROVINCIAL DE LA INFORMACION DE
CÁDIZ S.A

PLAZA MADRID S/N., EDIFICIO CARRANZA, FONDO
SUR, LOCAL 10,
C.P. 11010 CÁDIZ.

956 26 15 00

DATOS AUTOR

BRAULIO PAREJA MANZANARES

INGENIERO INFORMÁTICO

VIRGEN 5, CONIL, CADIZ
C.P. 11140

BRAULIO.PAREJA.MANZANARES@DIPUCADIZ.ES

FECHA DE PRESENACIÓN

JULIO 2017

FIRMA:

DURACION
ESTIMADA

600 HORAS

BRAULIO PAREJA MANZANARES

3. ESPECIFICACIONES DEL SISTEMA

3.1. Introducción

En este documento vamos a especificar los requisitos del proyecto, para ello abordaremos las necesidades que tiene EPICSA en monitorizar, mediante objetivos.

3.2. Objetivos

- Objetivo 1
 - El sistema debe tener recursos para garantizar el funcionamiento correcto del software.

OBJ-01	Elección del sistema administrador
Autores	Departamento de Sistemas y Redes
Importancia	ALTA
Descripción	Crear sistema con suficientes recursos y estable

Tabla 6: Objetivo 1

- Objetivo 2
 - El sistema debe de ser compatible con la mayoría de equipos que tiene la empresa y utilizar el agente más apropiado.

OBJ-02	Elección de agente
Autores	Departamento de Sistemas y Redes
Importancia	ALTA
Descripción	Instalar o activar agentes compatibles

Tabla 7: Objetivo 2

- Objetivo 3
 - Monitorizar anillo metropolitano para saber el estado que esta cada nodo en cada instante

OBJ-03	Monitorización de Anillo
Autores	Departamento de Redes
Importancia	ALTA
Descripción	Controlar el estado de las interfaces que generan el anillo metropolitano

Tabla 8: Objetivo 3

- Objetivo 4
 - Monitorizar los servidores del CPD para saber en cada momento que estado tiene el equipo

OBJ-04	Monitorización de CPD
Autores	Departamento de Sistemas
Importancia	ALTA
Descripción	Controlar el estado en el que se encuentra cada maquina

Tabla 9: Objetivo 4

- Objetivo 5
 - El sistema debe ser capaz de monitorizar las sedes remotas, tanto los servidores como los enlaces a la VPN e Internet

OBJ-05	Monitorización Ayuntamientos
Autores	Braulio Pareja Manzanares
Importancia	MEDIA
Descripción	El sistema ha de ser capaz de monitorizar las sedes remotas

Tabla 10: Objetivo 5

- Objetivo 6
 - Cuando suceda un acontecimiento significativo el sistema ha de ser capaz de avisarnos de manera inmediata

OBJ-06	Alertas
Autores	Departamento de Redes y Sistemas
Importancia	ALTA
Descripción	El sistema debe de alertar cuando suceda un evento

Tabla 11: Objetivo 6

- Objetivo 7
 - El sistema debe de facilitar la visión de las incidencias, que ocurran cuando está monitorizando.

OBJ-07	Interfaz amigable
Autores	Departamento de Redes y sistemas
Importancia	ALTA
Descripción	Interfaz amigable

Tabla 12: Objetivo 7

- Objetivo 8
 - Ha de ser capaz de tener distintas interfaces de usuario

OBJ-08	Privilegios de usuarios
Autores	Departamento de Redes y sistemas
Importancia	Media
Descripción	Capacidad para crear distintos usuarios

Tabla 13: Objetivo 8

- Objetivo 9
 - Para algunos monitores ha de ser capaz de generar graficas

OBJ-09	Graficas de estado
Autores	Departamento de Redes y sistemas
Importancia	Media
Descripción	Creación de grafico con la colección de datos

Tabla 14: Objetivo 9

3.3. Requisitos

- Requisito 1

- Se ha de disponer de un equipo para monitorizar

R-01	Servidor Dedicado y software
Autores	Departamento de Sistemas y Redes
Importancia	ALTA
Descripción	Equipo con prestaciones alta

Tabla 15: Requisito 1

- Requisito 2

- El sistema ha de funcionar 24/7

R-02	Disponibilidad
Autores	Departamento de Sistemas y Redes
Importancia	ALTA
Descripción	El sistema no puede caer

Tabla 16: Requisito 2

- Requisito 3

- Es necesario saber la capacidad de almacenamiento en cada instante

R-03	Capacidad de disco Servidores
Autores	Departamento de Sistemas
Importancia	ALTA
Descripción	Ver el total y la capacidad restante

Tabla 17: Requisito 3

- Requisito 4

- Es necesario saber la capacidad de memoria disponible

R-04	Memoria disponible en servidores
Autores	Departamento de Sistemas
Importancia	ALTA
Descripción	Ver el total y disponibilidad de la memoria

Tabla 18: Requisito 4

- Requisito 5
 - Tenemos que saber de cualquier equipo monitorizado cuando no está activo

R-05	Estado de los dispositivos
Autores	Departamento Sistemas y redes
Importancia	MEDIA
	El sistema ha de ser capaz de monitorizar las sedes remotas

Tabla 19: Requisito 5

- Requisito 6
 - Estado de las interfaces que crean las redes troncales tanto el anillo como las sedes externas

R-06	Estado de interfaces de Redes
Autores	Departamento de Redes
Importancia	ALTA
Descripción	Conocer el estado de la interfaz de red

Tabla 20: Requisito 6

- Requisito 7
 - Informar de los eventos a la personas adecuadas a través de e-mail y correo

R-07	Enviar alertas
Autores	Departamento de Redes y sistemas
Importancia	ALTA
Descripción	Informe de incidencias

Tabla 21: Requisito 7

- Requisito 8
 - Ha de ser capaz de tener distintas interfaces de usuario

R-08	Carga del procesador
Autores	Departamento de Sistemas
Importancia	Media
Descripción	Control del procesador

Tabla 22: Requisito 8

- Requisito 9
 - Saber el estado del internet

R-09	Estado de internet
Autores	Departamento de Redes
Importancia	Alta
Descripción	Monitorizar interfaces de con salida a internet

Tabla 23: Requisito 9

- Requisito 10
 - Controlar el estado del portal de la intranet

R-10	Monitorizar Web de la intranet
Autores	Departamento de Sistemas
Importancia	Alta
Descripción	Controlar si algún elemento de acceso a la intranet no funciona

Tabla 24: Requisito 10

- Requisito 11
 - Levantar servicios remotos automáticamente

R-11	Activar Servicios
Autores	Departamento de Sistemas
Importancia	Alta
Descripción	Capacidad de ejecución en maquina remota

Tabla 25: Requisito 11

- Requisito 12
 - Conocer todo momento la temperatura del CPD

R-12	Temperatura CPD
Autores	Departamento de Sistemas y Redes
Importancia	Alta
Descripción	Saber el estado y alertarnos de la temperatura del CPD

Tabla 26: Requisito 12

- Requisito 13
 - Distribuir los equipos por secciones en mapas

R-13	Mapas de distribución
Autores	Departamento de Sistemas y Redes
Importancia	Alta
Descripción	Distribución de monitores por zonas o grupos

Tabla 27: Requisito 13

3.4. Matriz de Rastreabilidad Objetivos / Requisitos

Mostraremos la matriz de rastreabilidad entre los objetivos marcados y los requisitos especificados.

	OBJ-01	OBJ-02	OBJ-03	OBJ-04	OBJ-05	OBJ-06	OBJ-07	OBJ-08	OBJ-09
R-01									
R-02									
R-03									
R-04									
R-05									
R-06									
R-07									
R-08									
R-09									
R-10									
R-11									
R-12									
R-13									

Tabla 27: Matriz de rastreabilidad

PROYECTO DE MONITORIZACIÓN DE LA GESTION DE SISTEMAS Y REDES DE LA EXCELENTÍSIMA DIPUTACIÓN PROVINCIAL DE CÁDIZ

CÓDIGO: IT5698929

CAPÍTULO 4: PRESUPUESTOS

DATOS CLIENTE

EMPRESA PROVINCIAL DE LA INFORMACION DE
CÁDIZ S.A

PLAZA MADRID S/N., EDIFICIO CARRANZA, FONDO
SUR, LOCAL 10,
C.P. 11010 CÁDIZ.

956 26 15 00

DATOS AUTOR

BRAULIO PAREJA MANZANARES

INGENIERO INFORMÁTICO

VIRGEN 5, CONIL, CADIZ
C.P. 11140

BRAULIO.PAREJA.MANZANARES@DIPUCADIZ.ES

FECHA DE PRESENACIÓN

JULIO 2017

FIRMA:

DURACION
ESTIMADA

600 HORAS

BRAULIO PAREJA MANZANARES

4. PRESUPUESTO

4.1. Introducción

En este documento, mostraremos el presupuesto necesario para abordar nuestro proyecto, el cual trataremos y descompondremos detallando los precios por componentes y servicios.

4.2. Presupuesto detallado

- Presupuesto Blade

Artículo	Unidades	P.V.P.	Precio Total
Dell PowerEdge 2950 Server Características: intel(R) Xeon(R) CPU X5460 @ 3.16GHz, 8 cores 16 Gb de RAM 160 Gb SSD	1	6456,32 €	6456,32 €
TOTAL			6456,32 €

Tabla 28: Presupuesto Blade

- Presupuesto Telefonía

Artículo	Unidades	P.V.P.	Precio Total
Modem Nokia TM-1	1	56,45 €	58,45 €
Duplicado Sim	1	9,99 €	9,99 €
TOTAL			68,44

Tabla 29: presupuesto Telefonía

Presupuesto Software

Artículo	Unidades	P.V.P.	Precio Total
ZABBIX 3.0	1	0 €	0 €
UBUNTU	1	0 €	0 €
SERVER 14.04 LTS			
TOTAL			0 €

Tabla 30: Presupuesto software

- Presupuesto mano de obra

Personal	Unidades	Horas	P.V.P./Hora	Precio Total
Personal Cualificado	1	600	18,75 €	11250 €
TOTAL				11250 €

Tabla 31: Presupuesto Personal

Este último gasto se podría abordar por personal de la empresa EPICSA contratado en plantilla

4.3. Presupuesto Global

- Total Presupuesto

Artículos / Servicios	Precio
Blade	6456,32 €
Telefonía	68,44 €
Software	0 €
Mano de Obra	11250 €
TOTAL	17774,74 €

Tabla 32: Resumen de Presupuesto

